

S. HRG. 111-821

**THE FINDINGS AND RECOMMENDATIONS OF THE  
DEPARTMENT OF DEFENSE INDEPENDENT RE-  
VIEW RELATING TO FORT HOOD**

---

---

**HEARING**

BEFORE THE

**COMMITTEE ON ARMED SERVICES**

**UNITED STATES SENATE**

**ONE HUNDRED ELEVENTH CONGRESS**

**SECOND SESSION**

—————  
**JANUARY 21, 2010**  
—————

Printed for the use of the Committee on Armed Services



Available via the World Wide Web: <http://www.fdsys.gov/>

—————  
U.S. GOVERNMENT PRINTING OFFICE

63-686 PDF

WASHINGTON : 2011

—————  
For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON ARMED SERVICES

CARL LEVIN, Michigan, *Chairman*

ROBERT C. BYRD, West Virginia	JOHN McCAIN, Arizona
JOSEPH I. LIEBERMAN, Connecticut	JAMES M. INHOFE, Oklahoma
JACK REED, Rhode Island	JEFF SESSIONS, Alabama
DANIEL K. AKAKA, Hawaii	SAXBY CHAMBLISS, Georgia
BILL NELSON, Florida	LINDSEY GRAHAM, South Carolina
E. BENJAMIN NELSON, Nebraska	JOHN THUNE, South Dakota
EVAN BAYH, Indiana	ROGER F. WICKER, Mississippi
JIM WEBB, Virginia	GEORGE S. LeMIEUX, Florida
CLAIRE McCASKILL, Missouri	SCOTT P. BROWN, Massachusetts
MARK UDALL, Colorado	RICHARD BURR, North Carolina
KAY R. HAGAN, North Carolina	DAVID VITTER, Louisiana
MARK BEGICH, Alaska	SUSAN M. COLLINS, Maine
ROLAND W. BURRIS, Illinois	
JEFF BINGAMAN, New Mexico	
EDWARD E. KAUFMAN, Delaware	

RICHARD D. DEBOBES, *Staff Director*

JOSEPH W. BOWAB, *Republican Staff Director*

# CONTENTS

## CHRONOLOGICAL LIST OF WITNESSES

### THE FINDINGS AND RECOMMENDATIONS OF THE DEPARTMENT OF DEFENSE INDEPENDENT REVIEW RELATING TO FORT HOOD

JANUARY 21, 2010

	Page
West, Hon. Togo D., Jr., Co-Chair, Department of Defense Independent Review Relating to Fort Hood .....	5
Clark, ADM Vernon E., USN [Ret.], Co-Chair, Department of Defense Independent Review Relating to Fort Hood .....	8
[Annex: The Report of the DOD Independent Review "Protecting the Force: Lessons from Fort Hood" follows:] .....	46



**THE FINDINGS AND RECOMMENDATIONS OF  
THE DEPARTMENT OF DEFENSE INDE-  
PENDENT REVIEW RELATING TO FORT  
HOOD**

---

**THURSDAY, JANUARY 21, 2010**

U.S. SENATE,  
COMMITTEE ON ARMED SERVICES,  
*Washington, DC.*

The committee met, pursuant to the notice, at 9:30 a.m. in room SD-G50, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Lieberman, Reed, Akaka, E. Benjamin Nelson, Hagan, Burris, Kirk, McCain, Inhofe, Chambliss, Thune, LeMieux, Burr, and Collins.

Committee staff members present: Richard D. DeBobes, staff director; and Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Gabriella Eisen, counsel; Jessica L. Kingston, research assistant; Gerald J. Leeling, counsel; Peter K. Levine, general counsel; Jason W. Maroney, counsel; and William K. Sutey, professional staff member.

Minority staff members present: Diana G. Tabler, professional staff member; and Richard F. Walsh, minority counsel.

Staff assistants present: Kevin A. Cronin, Paul J. Hubbard, and Jennifer R. Knowles.

Committee members' assistants present: James Tuite, assistant to Senator Byrd; Vance Serchuk, assistant to Senator Lieberman; Carolyn A. Chuhta, assistant to Senator Reed; Nick Ikeda, assistant to Senator Akaka; Ann Premer, assistant to Senator Ben Nelson; Juliet M. Beyler and Gordon I. Peterson, assistants to Senator Webb; Jennifer Barrett, assistant to Senator Udall; Roger Pena, assistant to Senator Hagan; Roosevelt Barfield, assistant to Senator Begich; Nathan Davern, assistant to Senator Burris; Ron Carlton, assistant to Senator Kirk; Anthony J. Lazarski, assistant to Senator Inhofe; Lenwood Landrum and Sandra Luff, assistants to Senator Sessions; Clyde A. Taylor IV, assistant to Senator Chambliss; Adam G. Brake, assistant to Senator Graham; Jason Van Beek, assistant to Senator Thune; and Molly Wilkinson, assistant to Senator Collins.

**OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN**

Chairman LEVIN. Good morning, everybody. The committee meets this morning to consider the findings and recommendations of the independent panel appointed by the Secretary of Defense fol-

lowing the tragedy at Fort Hood. The primary objective of the panel was to “determine whether there are programs, policies, or procedural weaknesses within the Department of Defense (DOD) that create vulnerabilities to the health and safety of defense employees and their families.”

Today’s open hearing is on the panel’s unrestricted report. A restricted annex to their report titled “Oversight of the Alleged Perpetrator,” focuses on information which in the judgment of DOD could prejudice a criminal prosecution if it were discussed in public. We’ll have a closed session after this open hearing has concluded.

Our witnesses this morning are Togo West, former Secretary of the Army, and Admiral Vernon Clark, U.S. Navy-Retired, former Chief of Naval Operations, who together co-chaired this independent review. We have reviewed their unrestricted report. Members have had an opportunity to review the restricted annex. We welcome you both. We thank you for returning to government service for this very important task. It’s a continuation of your great patriotism and loyalty.

On the afternoon of November 5, 2009, an Army field-grade officer, Major Nidal Hassan, opened fire on fellow soldiers in the Soldier Readiness Center at Fort Hood, TX, killing 12 soldiers, 1 civilian, and wounding or injuring 43 others. There is information in the public domain indicating that this tragic and violent incident was preceded by a number of indicators that would seemingly raise questions about Major Hassan’s fitness to serve as an officer and Army psychiatrist. Some of those indicators were email contact with a radical Muslim cleric in Yemen, concerns about his expressed belief that sharia religious law took precedence over the U.S. Constitution, presentations that he made that for some of the witnesses indicated sympathy for violence, and concerns expressed by superiors and peers about his duty performance and his ratings.

So there’s a connect-the-dots issue here. There are a number of other investigations that will examine the failure to connect those dots. That is not part of today’s open hearing. DOD’s inquiry is one of several inquiries that are or will be examining the incident. The President has directed a review of intelligence matters related to the shooting, the Federal Bureau of Investigation (FBI) is conducting a review of its procedures, and a military justice investigation is ongoing.

The review that we will consider today was a first assessment of the Department’s policies and procedures to identify gaps that warrant further investigation and action. Clearly there is much more that needs to be done. The Secretary of Defense has committed to tasking each Service and pertinent DOD agencies to conduct an in-depth follow-on review based on the findings of this report.

The Secretary of Defense gave this independent panel less than 60 days to conduct a quick-look review “to identify and address possible gaps and/or deficiencies in 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, the sufficiency of DOD’s emergency response to mass casualty situations at DOD’s facilities, and the response to care for victims and families in the aftermath of a mass casualty situation, and, finally, the execution and adequacy

of Army programs, policies, and procedures as applied to the alleged perpetrator.”

The panel completed its work and delivered its report to the Secretary of Defense on time, and that is remarkable, given the short period of time over the holidays that the panel was given for this task. This could only be done under the strong leadership of our witnesses, who co-chaired the independent panel.

A copy of the report of the DOD Independent Review titled: “Protecting the Force: Lessons from Fort Hood,” will be included in the record of this hearing.

[The information referred to follows:]

[See Annex.]

Chairman LEVIN. The independent panel made a total of 42 findings with associated recommendations in the basic report, with an additional 12 findings in the restricted annex. The panel gives Fort Hood high marks for a quick and effective response to this incident, while recognizing that DOD can and should do more to prepare for multiple simultaneous incidents in the future.

The panel found that some programs, policies, processes, and procedures were adequate, but were not complied with, and other policies are in need of revision to give commanders the tools that they need to counter internal threats as well as new threats that may manifest themselves in the future.

The report produced by this independent panel gives DOD a blueprint for additional reviews and resulting policy changes. For instance, the Department will need to evaluate and update policies and procedures for identification of indicators of violence, clarify policy regarding religious accommodation, review and improve military personnel records, and refocus defense force protection programs on internal threats.

This committee has a continuing interest in the findings, recommendations, and changes made based on these reviews. It will continue its oversight of DOD actions, and I assume this will be the first of a number of hearings into this incident, how it could have been avoided and how we can deter similar tragedies in the future.

Before I close, I want to commend the soldiers, the first responders, the law enforcement personnel, and the health care providers for their prompt, professional, courageous acts that prevented an even greater loss of life as a result of this horrendous act.

I would also like to insert for the record Senator Burriss’ statement.

[The prepared statement of Senator Burriss follows:]

PREPARED STATEMENT BY SENATOR ROLAND W. BURRIS

Thank you, Mr. Chairman, and welcome Secretary West and Admiral Clark. I am again pleased with both of your taking on this most important effort to look at the lessons learned as a result of the tragedy at Fort Hood. The Nation, and more importantly, the families, are looking to all of us to make sense of this situation and provide them with answers and solutions to ensure that this type of incident does not occur in the future. The members of our military have performed, and will continue to perform, their duties with honor and integrity, and it is incumbent upon us to provide them the guidance and oversight that they deserve.

I thank you for your testimony and your service to the Nation.

Chairman LEVIN. Senator McCain.

**STATEMENT OF SENATOR JOHN MCCAIN**

Senator MCCAIN. I thank you, Mr. Chairman, and I join you in welcoming Secretary West and Admiral Clark, and I thank them for their continued service to their country, and I thank them and their staff for their work in conducting this independent examination of the tragic events last year at Fort Hood.

I agree with the statement in your report that “the events of November 5, 2009, are first and foremost a tragedy for all involved; families, colleagues, and the Nation.” My thoughts and prayers continue for the families and friends of the victims of this terrible tragedy.

I appreciate that DOD initiated this review to scrutinize itself with regards to organizational shortcomings that led to the horrific killings of 12 servicemembers, 1 Army civilian, and the wounding of 43 others. However, most of your report is devoted to personnel policies and emergency shooting response procedures. The report concentrates on actions and effects, rather than the motivations. But it was motives that led to the Fort Hood killings that should have been examined, whatever the political correctness implications. The panel’s effort to assist DOD and the American people to understand the threat to national security and to our military personnel was undermined as a result.

We have a profound responsibility to try to prevent harm to all Americans, especially those who volunteer for service in the Armed Forces and have, as a result, become high-value targets for our enemies. I find insufficient information in this report to advance the identification and elimination of this threat.

The omission in your report of adequately recognizing and addressing the specific threats posed by violent extremism to our military servicemembers is troubling. We owe it to our servicemembers and their families to be very candid in addressing the threat of violence driven by violent Islamic extremism.

I believe General Jack Keane, the former Vice Chief of Staff of the Army, made the point clearly in his testimony on November 19, 2009, when he said that: “We need to provide a service to all Muslims serving in the Armed Forces by clearly describing the threat, explaining the indicators of potential problems, and obliging all military personnel to report individuals who display these beliefs and actions.”

I believe the information you have compiled in the restricted annex to this report regarding failures in the performance of officers who supervised Major Hassan during his medical education will help to ensure accountability and corrective measures. Much of this information, not surprisingly, has been leaked to the media and it portrays a system badly in need of reevaluation and reform.

I expect the Secretary of the Army to move quickly to ensure accountability for the shortcomings you identified and to demand more from our officers and organizations. They should have the courage and integrity to identify substandard officers who represent potential threats to those around them. I hope you can comment today on what we can expect in this regard.

I also believe that your findings and recommendations will have value in prodding DOD and the Services to take on the challenge of identifying the legal and regulatory barriers to information-shar-

ing called for in the report. There is an array of concerns that must be addressed in this regard. Concerns about individual privacy, threat of litigation, equal opportunity violations, First Amendment rights, medical privacy, including stigma from seeking treatment, and abuse of authority are just a few. They represent a Gordian Knot that has to be cut.

What happened at Fort Hood was something more than an isolated incident, more than a random act of violence by an alleged perpetrator. It was a terrorist act, struck against us as part of the broader war in which we are now engaged. Without focusing on the threat posed today by violent Islamic extremism to our military and their families, we can't address those vulnerabilities and correct them.

I thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator McCain.

Now let me call on you, Secretary West.

**STATEMENT OF HON. TOGO D. WEST, JR., CO-CHAIR, DEPARTMENT OF DEFENSE INDEPENDENT REVIEW RELATING TO FORT HOOD**

Mr. WEST. Thank you, Mr. Chairman, Senator McCain, and distinguished members of the committee, for the opportunity to testify before you on this important matter. I wonder if I might do one or two quick housekeeping things. You have from us our written opening statement. It is a joint statement by both Admiral Clark and by me, and we would ask you to include that in the record.

Chairman LEVIN. It will be.

Mr. WEST. With that, we will give a few comments, a bit of a roadmap to what's in our report, although we're aware that you have had a chance to look through it. I will do the first group and then, if you will permit, Admiral Clark will take up from there.

Chairman LEVIN. That would be fine. Thank you.

Mr. WEST. As you pointed out, Mr. Chairman, and you also, Senator McCain, that day—November 5, 2009—was a day of tragedy, and we will all remember it as such. Out of that tragedy, there are some instructive lessons for us, and those are what we address in our report.

As you pointed out, Secretary Gates was specific in what he asked us to do, contained both in a memorandum to us in his terms of reference and in his statement at his press conference. That is important to us because it bounds our undertaking, as did the time within which we were asked to complete our work, and also as did the fact that he had already indicated his intention to have a lengthier, more in-depth follow-on review of both our report and the issues that we raise by the Services. He has already begun the process of referring the report out for their follow-on activities.

As you pointed out, we were asked to look at personnel policies, specifically those that pertain to our ability to make identifications of those who are a risk, a danger to their fellows in the Service, to look at how those policies, practices, and procedures allow us to deal with, after we have identified those threats, and look at the ways in which there are gaps or deficiencies—his language—that we need to improve upon going forward.

He also asked us to look at force protection measures with the same idea, not just in the Army, but across the board in DOD, and the Office of the Secretary of Defense (OSD) procedures and regulations at the level of every Service.

Third, to look at our preparations and our policies concerning preparations for mass casualty events and for responding to them.

Finally in that group of four, to look at how we provide for the support of those who provide needed medical care to those who serve.

The fifth assignment that he gave us was a very specifically stated one and it's in one of the annexes to our report, and that is this: to examine the Army's application of its procedures and policies to the alleged perpetrator. I make that distinction because he did not ask us to go and explain what happened, although it certainly, I think, would appear to all of us, you and we as well, that without an understanding of what happened we certainly couldn't understand how the Army applied its policy. But our purpose, our direction, was to understand the Army's application of its policies and procedures to the perpetrator. That is what is contained in our annex 5.

I should say to you as part of an understanding of how we organized and prepared for this that that was, in our view, going to be simply chapter 5 of a report that we would submit to you today for review. After review, departmental lawyers concluded, and I think they concluded properly, that there was a great risk of interfering with the military justice, the criminal proceeding, and that is why it is submitted to you as a restricted annex.

With that in mind, we were told not to interfere with the intelligence investigation that had proceeded, nor with the military justice, nor with the ongoing parallel FBI review, and we've made an attempt not to do so. What we did do was to organize ourselves into five teams, supported by personnel whom we requested and were assigned to us from the military departments and from OSD. Each of these teams looked into the specific areas that we have described in the report, submitted their report of their activities to us, and Admiral Clark and I and those who worked directly with us, took responsibility for reviewing and stating our conclusions and our views with respect to that.

Our personal views are found throughout the report, but they are specifically called out in the executive summary, which you note we took the step of signing ourselves so that you would know that the words of the executive summary come from us, including those five or six recommendations that are for specific early action by the Secretary of Defense. Let me report that he has already taken some of those actions as we speak.

We also had a board of advisers drawn from the senior ranks of the Department, the military ranks, whose purpose was not to lead a team, although two of them were team leaders, but merely to review as we went and provide an overall perspective of what we were looking at and how we were stating it and how it would affect real progress for the Department in terms of responding to what had happened. Their help to us was invaluable, because when you think about it, otherwise the Admiral had himself and me to

bounce these things bounce and forth, to discuss. The board of advisers gave us an additional group with the same broad range.

A word or two at this point from both Admiral Clark and me about the actual landscape of the report. What you have before you has five chapters with an executive summary at the front and with some annexes. The first chapter is a very brief, one-page synopsis that we thought we could state in a public report, that is much more dealt with in detail in the annex, and that is about the alleged perpetrator.

Chapters 2, 3, 4, and 5 are the bulk of what the Secretary asked us to look at. I call your attention to chapter 2, which is about the personnel policies, which is divided into three sections, one having to do with how we identify the kinds of things that can lead a person to become a danger to his or her colleagues. A second part of it has to do with sharing that information, getting it to the right place. I point out to you that in our finding 2.2 in that report we acknowledge a specific difficulty and that is the fact that information that is obtained in one place does not always go forward with a servicemember to successive assignments, thus making it difficult for commanders to know exactly what they're dealing with. The third section in chapter 2 has to do with barriers to action.

Three observations before I ask your permission to have Admiral Clark take on the description to you of other parts of the report. The first is this: There can never be too much preparation. In some ways, we could say that no matter how much preparation you've done there is more that could be done. At Fort Hood, the leaders had anticipated mass casualty events in their emergency response plans, and it showed in their responses. As you have acknowledged, Mr. Chairman, and as also did Senator McCain, the response was prompt. Within 2 minutes and 40 seconds of the first 9-1-1 call, first responders were on the scene of the shooting, and by first responders I mean elements of the Fort Hood security forces. Within a minute and a half after that, the assailant had been taken down, and within 2 minutes and 50 seconds after that two ambulances and an incident command vehicle from the post hospital had arrived to begin to dispense needed medical care.

Lives were saved. Yet, as you have pointed out, 13 people died and scores others, 43, were wounded. We must prepare better, plan more intensively, and take the hard effort to look around the corners of our future to try and anticipate the next potential incident.

Second, we must be attentive to today's hazards. Today the requirement that is imposed upon us in DOD is to understand the forces that cause an individual to radicalize, to commit violent acts, and thereby to make us vulnerable from within.

Finally, the thread through all of this is violence, how do we detect the indicators of violence, how do we share the information about those indicators, and then whether we have the foresight to act.

Thank you, Mr. Chairman, and with your permission Admiral Clark will take it from here.

Chairman LEVIN. Thank you so much, Mr. West.  
Admiral.

**STATEMENT OF ADM VERNON E. CLARK, USN [RET.], CO-CHAIR, DEPARTMENT OF DEFENSE INDEPENDENT REVIEW RELATING TO FORT HOOD**

Admiral CLARK. Good morning, Mr. Chairman. I appreciate the opportunity to be with you today to talk about the work of Secretary West and myself and the group of people who worked with us in this effort.

Let me make a few comments and get right to the questions. I know that you have questions for us, so first let me talk about force protection for a moment. The principal message of our review with regard to force protection is simply this: There are lots of policies on force protection inside DOD. Since September 11, we have built many barriers. However, existing policies simply are not optimized to deal with the insider threat, the evolving threat that we see today—and when people talk about the new threat, we’re talking about the insider threat.

Now, complicating the entire force protection challenge is the diverse nature of the way DOD has evolved since September 11, 2001. So one of our recommendations to the Secretary was that you have to look at the organization itself. On page 25 of the base report, you find a description of the various Under Secretaries and Assistant Secretaries of Defense that are charged with responsibilities for working the force protection challenge. Synchronization is difficult and, simply stated, no senior DOD official is assigned overall responsibility for synchronizing this policy.

Notice, I’m not saying that one person should have all that responsibility. Neither is Secretary West. We were careful not to define the specific organization for the Secretary of Defense. Our observation is synchronization is pretty difficult the way it’s set up, the way it is today, and we recommend that it be looked at. The key point, too, is that there has to be a mechanism in place to do this integration, and that’s our recommendation.

Second, the task of identifying employees who potentially could threaten the workforce—and I ask us to remember that the Secretary asked us to look at violence. So the question is, how do we identify individuals who have the potential for violent behavior. Certainly in our research we found that detecting a trusted insider’s intention to commit a violent act requires observation skills that may not be in place. This is the evolving threat.

So there’s a requirement to understand behavioral cues and anomalies that would alert commanders and supervisors to know that such a threat exists. While DOD focuses very effectively on many things, there is insufficient knowledge and guidance concerning who this insider threat is: Who are these people? There is insufficient guidance on workplace violence and, most importantly, how to identify the person who has the potential to self-radicalize. In our view it is simply insufficient.

The key word here is “violence.” Now, since our report has come out some have criticized us for not suggesting and talking enough about violent Islamic extremism. When we talk about self-radicalization, and the term appears numerous times in our report, we’re talking about the behaviors that create and lead to violence. That’s what we’re talking about. The lack of clarity for comprehensive indicators limits the commanders’ and supervisors’ ability to

recognize the potential threats. Fixing this issue will be critical to solving this problem in the future.

DOD policy on prohibited activities—and I have the instruction here with me that talks specifically about what prohibited activities are inside the Department—this instruction in our view is too limited and it only addresses active and very visible participation in groups that may pose threats to good order and discipline inside the ranks.

So we found that this lack of clarity for comprehensive indicators which limit commanders' and supervisors' ability to recognize the potential threats—we're talking about people who could hurt themselves. The Secretary of Defense cited specifically, people could hurt themselves, for example the issue of suicide, criminal and gang behavior, people that are advocating supremacist doctrine, family violence, evolving threats like self-radicalization—identifying these key indicators is critical to focusing the force on the threat.

Let's talk about information sharing. Secretary West addressed it also and let me just make a couple of points. The policies governing information exchange inside the Department and in the intergovernment system, in our view the policies are deficient. They do not support detection and mitigation of the internal threat.

DOD and Service guidance does not provide for maintaining and transferring relevant information from one duty station to the other. Now, remember we're doing phase one of this. As you talked about, Mr. Chairman, we did this review in a hurry. That's what the Secretary of Defense wanted us to do. Thousands of pages of review, but put the spotlight on the things that the Services can fix in a hurry. It is our view that this internal information exchange has to be examined.

In other words, how can commanders connect the dots if they don't have some information that's maintained at a local level and hasn't transferred from one command to another. I will tell you that automated systems inside the Services do not allow them to share information on, for example, registered users and persons who routinely come and go from a base and may become a threat.

So the issue of maintaining and transferring all of the relevant information, information that could lead to the identification of contributing factors, that's the issue.

Last Friday, the Secretary of Defense, in his press conference, stood and addressed his observations about our report. One of the things that I was happy to see him address was his comment that Secretary West and I are of the view that we have to become more adaptable and certainly we have to be proactive, but we have to be able to adapt rapidly to this changing security environment, bringing a wide and continuously evolving range of tools, techniques, and programs into play.

I just want to emphasize that there's no single-point solution for this evolving threat. We have to keep working at it. We need architectures and structures in place that will make that possible.

One other point about information sharing. Certainly robust information sharing is essential. Hand in glove with that information sharing is the required command and control apparatus, be it systems, policy, doctrine, tactics, techniques, and procedures, to convert this information into timely decisions and actions.

The bottom line, Mr. Chairman, members of the committee: We have to remove the barriers, all of the barriers. We have to equip and enable the commanders, people in decisionmaking positions, their ability—Mr. Chairman, you used the phrase—to connect the dots. We have to get the information and thus the indicators to the appropriate level of people in command.

Just a couple of comments about emergency response. Secretary West addressed this. Mr. Chairman, you also certainly did justice to the brilliance of the people at Fort Hood and their actions. Lots of good news related to the emergency response.

Mr. Chairman and members, I just wanted to try to put this in perspective. I committed my life in service for 37 years. I created in those 37 years a number of lessons learned myself, and I heard dozens of lessons-learned reports. On the second day that our team was in existence, Secretary West and I got on a plane with a few members of our team and we went to Fort Hood. We walked the ground and they showed us the space where all of this happened and looked at the terrain. Then we sat down with General Kohn and his command team and they gave us this presentation that had been turned in a matter of a few days, their lessons learned. I want to tell you that I was really impressed.

So I heard a lot of them in my 37 years and I want you to know that I never ever heard a better one than I heard at Fort Hood that day. The base personnel were ready to respond. They had trained at this, they had worked at it. Secretary West talked about the timeline response to the active shooter. It was brilliant.

All of that said, it still could have been better, and in our review we found areas where it could be better. In their own lessons learned they identified areas where it could be better. I spoke in the last subject about the command and control system. They need a better system. General Kohn had to deal with misinformation, and should anybody be surprised? I don't think so. There's never been a crisis ever that there wasn't misinformation. Being able to deal with it in a rapid way and being able to deal with a potential multiple event, Mr. Chairman, as you indicated, is critical.

Fundamentally we believe that we can improve by providing a well-integrated means to gather and evaluate and disseminate the wide range of information that will make it possible for commanders to perform to the maximum.

This report is about focusing on better tools for commanders. This report is about focusing on violence prevention, in whatever form that violence manifests itself. This report is about adapting and evolving to rapid change, sharing information, connecting the dots, and exercising against the most stressing and pressing scenarios that we know how to present, so that we satisfy ourselves that we are able to perform to the standards that we have identified ourselves.

I want to close by just acknowledging my alignment with all the comments that have been made about the people at Fort Hood, the families that have suffered loss, and just say that the thrust of our work has been to do everything that we know how to do to identify policies, procedures, practices, and programs that can be made better, so that the U.S. Armed Forces continue to be the outstanding force that it is today.

Thank you very much, Mr. Chairman, and I look forward to your questions.

[The joint prepared statement of Mr. West and Admiral Clark follows:]

JOINT PREPARED STATEMENT BY HON. TOGO D. WEST, JR. AND ADM VERNON E. CLARK, USN (RET.)

Chairman Levin, Senator McCain, distinguished members of the committee: We appreciate the opportunity to appear before you and discuss the findings and recommendations of the Department of Defense Independent Review Relating to Fort Hood.

Two months ago, a gunman opened fire at the Soldier Readiness Center at Fort Hood, TX. Thirteen people were killed and 43 others were wounded. November 5, 2009 will be remembered as a day of great tragedy. We extend our deepest sympathy to the families of the fallen, to the wounded, to their families, and indeed all touched by this tragic event.

Following the shooting, Defense Secretary Robert M. Gates established the Department of Defense Independent Review Related to Fort Hood, and asked that Admiral Clark and I lead it. We have done so and report on it today. 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. The challenge for the Department of Defense (DOD) is to prepare more effectively for a constantly changing security environment. It is with that backdrop in mind that Secretary Gates asked us to conduct our review.

Secretary Gates charged us to provide an independent review and assess whether there are programs, policies or procedural weaknesses within DOD that create vulnerabilities to the health and safety of our service men and women, DOD civilians, and their families. Dr. Gates asked that we take a careful look at personnel policies, force protection measures, emergency response procedures and support to our military health care providers. He asked us to evaluate the Army's application of its policies, programs, processes, and procedures to the alleged perpetrator.

We established a board of advisors with senior officers from the four Services. We constituted five review teams, consisting of a range of experts, who investigated the key tasks outlined in our terms of reference. The teams had unrestricted access to personnel and facilities. The teams traveled to Fort Hood as part of their review.

Our charter directed us to focus on the noncriminal aspects of the shooting. Although Fort Hood was central to our review, our scope extended across the entire Department in order to gather the most significant and meaningful findings and recommendations. 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 limited the depth of our report in areas that will be covered in follow-on reviews.

We recently submitted our report to the Secretary of Defense. Before discussing the overall report, we note that we cannot address specifics with respect to the alleged perpetrator in open session, in order to preserve the integrity of the ongoing military justice process. We can tell you, however, that several individuals failed to apply professional standards of officership regarding the alleged perpetrator. We recommended the Secretary of Defense forward these issues of accountability to the Secretary of the Army. The detailed results and findings associated with the alleged perpetrator are found in a restricted annex that will not be publically released at the present time.

The review was much broader than the assessment of the alleged perpetrator. With that in mind, our report includes recommendations to strengthen DOD's ability to prepare for and respond to potential threats. It is based upon research by our teams of more than 35,000 pages from over 700 documents related to departmental policies, programs, processes, and procedures.

Before discussing the details of our findings, we would like to highlight some observations from the tragic events on November 5.

First, no amount of preparation is ever too much. Leaders at Fort Hood had anticipated mass casualty events in their emergency response plans and exercises. The initial response to the incident demonstrated this. It was prompt and effective. Two minutes and 40 seconds after the initial 9-1-1 call, Fort Hood first responders arrived on the scene. One-and-a-half minutes later, the assailant was incapacitated, taken into custody, and remained in custody handcuffed to a law enforcement representative for the next several chaotic hours. Two ambulances and an incident command vehicle from the post hospital arrived on the scene 2 minutes and 50 seconds

later to begin providing lifesaving emergency care. Yet 13 people died; scores were wounded. We will prepare harder; plan more diligently; seek to envision the next incident.

Second, we must be attentive to today's hazard. Even as the role of our nation's military is to confront the external threat to our country, one of the most significant emerging concerns in the protection of our force is the internal threat. We need to develop a better understanding of the forces that cause a person to become radicalized; commit violent acts; and make us vulnerable from within.

Third, courage and presence of mind in the face of crisis can carry the day. It happened at Fort Hood. Courageous acts were the key to preventing greater losses that day.

As our report reveals, however, these attributes alone are not enough to protect our force. We must exercise the foresight necessary to identify the looming menace—self radicalization and its often resultant violence—and act preemptively.

Our review of DOD policies, procedures, and processes revealed shortcomings in the way DOD is prepared to deal with internal threats, and in particular, the threat posed by troubled and potentially dangerous individuals and groups.

Commanders are our key assets to identify and monitor internal threats. Existing policies, however, are not optimized for countering these threats. The policies reflect insufficient knowledge and awareness required to help identify and address individuals likely to commit violence.

While the department focuses very effectively on many things, guidance concerning workplace violence and the potential for self-radicalization is insufficient. DOD policy on prohibited activities is limited and only addresses active and visible participation in groups that may pose threats to good order and discipline. This lack of clarity for comprehensive indicators limits commanders' and supervisors' ability to recognize potential threats and detecting a trusted insider's intention to commit a violent act requires observation of behavioral cues/anomalies.

Complicating the force protection challenge is the diverse nature of responsibilities as they have evolved within DOD since September 11. Because no senior DOD official is assigned overall responsibility for force protection policy, synchronization is difficult. Moreover, there is a lack of DOD policy integration. This has resulted in a lack of a well-integrated means to gather, evaluate, and disseminate the wide range of behavioral indicators that could signal an insider threat. Some policies governing information exchange, both within DOD and between outside agencies, are deficient and do not support detection and mitigation of internal threats. The time has passed when 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.

As the Secretary indicated, we see a requirement to create the ability to adapt rapidly to the changing security environment, which requires anticipating new threats and bringing a wide and continuously evolving range of tools, techniques, and programs into play. Robust information sharing, therefore, is essential, along with the accompanying command and control structure to convert active information gathered on potential threats into decisions and actions, including dissemination of the analysis and assessments 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. Real-time information sharing will be critical should we face a situation of multiple events.

While all 50 States have complied with the Federal requirements for the National Incident Management System, designed for a synchronized response in crises, there are no established milestones to define initial and full capability within DOD. The timelines should be evaluated; doing so could lead to an umbrella plan for emergency response and recovery and ensure interoperability with all the States. Synchronizing the DOD emergency management program with this national guidance will ensure the Department can integrate effectively with all partners in response to any and all emergencies. Using common emergency management principles, we can prepare our military communities to respond to emergency from the smallest incident to the largest catastrophe.

The response by the Fort Hood community in the aftermath of this tragedy serves as a reminder of the strength, resiliency and character of our people. We were very impressed with them, both military and civilian. In a community where we might have expected the fabric of trust to fray, it remained intact and grew stronger through mutual support. The thrust of our effort has been to do all that we can to prevent similar tragedies in the future.

Chairman LEVIN. Thank you, Admiral. Thank you both very much.

Let's try an 8-minute first round. The panel found that "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." I think what you're saying is that, obviously, this country believes in tolerance of others' religions, but it can never be tolerant of violent radical views that are dressed up in religious garb. I think that's that point reworded.

I couldn't agree with you more. Sometimes views that are clearly either inherently violent or promote violence are dressed up in religious clothing, and that automatically means that people who are sensitive to others' religious views then are put on the defensive right away, or reluctant right away to point out what is underneath the claim of religion.

So the line has to be there. Obviously, we want to continue our tolerance, but we have to be much harder and much more intolerant of views that are radical, promote violence, or encourage violence.

So my first question to you is about the policy of the Department, which is limited to and addresses only active participation in groups that pose threats to good order and discipline, is far too narrow a policy because of the self-radicalization point—you don't have to participate in a group that poses that kind of a threat to be a threat yourself. My first question is how would you—and I know you're not here to provide remedies and that wasn't your job, but I assume that you agree that it's not just that that policy should be examined, but that in your judgment at least it's just simply too limited a policy. I'm wondering whether or not, for instance, you would agree that communication with a radical cleric who promotes violence is the kind of conduct that should raise real questions. Would you agree with that, even though it's not active participation at that point? It's just simply communication, asking someone for their recommendations and views. Would you agree that that ought to be raising great suspicion, without getting into this particular case?

Mr. WEST. Mr. Chairman, I would certainly agree. I think we both would. I think your larger point that this is an example of, we would agree with as well, and that is that, yes, in the past perhaps membership alone in a group may have been less looked upon than the actual act of doing things, but in this environment we have to look at the group. We have to understand its purposes.

It is already considered by some that there is a tool that enables a commander to declare certain kinds of action, including that, a threat to his immediate area's good order and discipline. But we think DOD can just simply strengthen the ability of commanders to look at and example exactly what kind of activity they are permitting and whether or not we can better define it.

Membership in a group that has a record of active advocacy of violence, as well as your point, communication, especially repeated communication—again, not referring to any particular case—with those who advocate violence, those are all signals that we need to be able to indicate in our publications and in our regulations commanders are authorized to look at and react to.

Chairman LEVIN. Even if there weren't active participation or communication with radical persons who are promoting violence, even if there's simply the expression of views which promote violence without any information about participation in a group or communication with radical extremists—if somebody gets up and says, "I believe that the Constitution comes in second and that my religious views come in first," would that not be that kind of a signal which ought to indicate some real genuine concern? Would you agree with that?

Admiral CLARK. I certainly do agree with it. It goes without saying that where we draw our red lines is a very, very important point. But you know, if you look at our history, we as a people as Americans have always been very careful about where we draw those lines.

I so appreciate your introduction to this question by your comments about that we are a tolerant people. When I look at the DOD instruction here, it talks about what people can do when they're at work and things that they can't do at work, but they can do on their private time. What we're suggesting is that we have to better understand how people go through this process from being a non-radicalized person to radicalization and what does it mean.

So I align with your comments completely. I want to make one other observation, Mr. Chairman. In our report, we talk about Active Duty members of the military, but DOD is much broader than just the Active Duty people in uniform. We understand that when Americans raise their right hand and take a pledge to serve in the Armed Forces that there are some freedoms that they set on the shelf. The challenge that we're facing here in security applies to everybody in DOD, and that includes civilians, contractors, and a whole other body of people.

Then you could look at this and say, "this is not just DOD; this is the whole of our Nation; and the whole of government." This is a real challenge that we face.

Sir, you made the comment, when a shipmate hears a comment that's being made that is approaching a defined red line or crossing a defined red line, that we must make sure our people understand where those red lines are. That means we must have a very effective education program and outreach program, that people understand this is about our own security and the right to self-defense is absolutely not in question. We have the right to do that.

Chairman LEVIN. People should not be afraid of reporting information that they believe in their good judgment represents a potential threat to good order and discipline and to the safety of the country or of their own group out of fear that that might be viewed by some as being intolerant of religious views. We have to simply allow people the freedom to report something which they believe is a threat to their group, their country, or to the individual himself or herself, and not be dissuaded by the fact that the views are dressed in some religious garb.

Admiral CLARK. Good order and discipline is the fabric upon which the greatness of the U.S. military is built, and we have to ensure that we do everything we know how to do to protect it.

Chairman LEVIN. Secretary West, did you want to add anything to that?

Mr. WEST. No. I think the Admiral caught the point I would have made, which is that we are sensitive to the fact that we are talking about expressions and expressions in many cases that pertain to religion—two different hits on the First Amendment. But as he pointed out, when a member takes an oath of office there are some things as to which he or she agrees to be regulated. We believe that where there is a clear connection with a potential for violence that would cause damage to one's fellows in the Service, this is a basis on which we can encourage the Department to act more clearly and more aggressively.

Chairman LEVIN. My final question is this. You have not been given the charge of recommending remedies for where there are gaps. That's not part of your charge, although you freely responded to my questions this morning and I appreciate that. Who is in charge of responding with remedies to your recommendations? What is the timetable? Does this go right up to the Secretary of Defense and has he assured you that he will consider appropriate remedies within a certain timetable, or is there somebody else in the Department that's on the remedies side of what you've outlined here?

Mr. WEST. The answer to your question is twofold. I'll take the second first, which is: Yes, in his follow-on review he is ordering two sets of things. He's in that process. I think some orders have gone out, but not others. One, he is going to ask a single member of his staff—we believe, but we don't want to commit him—it is his prerogative, not ours—perhaps the Assistant Secretary for Homeland Defense or Security—I'm not authorized to make that statement, don't know, but that's our belief—to conduct a follow-on review, but each of the Services also.

Part of their job is to take this report—he will refer it to them—and to provide their recommendations as to how to implement. That's the answer to your second question.

The first answer is in some ways you give Admiral Clark and me too much of a bye. The fact is his direction to us was to come up with action memo recommendations as well.

Chairman LEVIN. All right. In that case, I withdraw that comment. Are your recommendations then to be acted upon in a certain length, period of time?

Mr. WEST. I'm not clear.

Chairman LEVIN. What I'm referring to is this. You say that there's inadequate clarity on the issue we've been discussing. The recommendation is a general one: Provide clarity. But it's not the specific clarity. It's just: You should provide clarity, Mr. Secretary. I couldn't agree with you more, but it's not what the new regulation should be. That's going to be left up to the Secretary. That's what I meant when I said you have not provided the specific new language that should be in place replacing the unclear language. That's what I meant by that.

Now, is there a timetable?

Admiral CLARK. Yes, there is. There is a timetable, he announced it Friday.

Chairman LEVIN. What is it?

Admiral CLARK. He wants first impressions back in March and he wants to wrap this up by June.

If you read the language, we were very careful with our recommendations. First of all, you confirm the Secretary of Defense and that allows him to be the person who makes policy. We were very aware of the fact that at one point in our lives we were those people, but we're not those people today.

So we suggested on numerous occasions he review policy because we thought there were holes or weaknesses or gaps. There were some places that the language is slightly stronger: It's absolutely clear to us that the policy is—and we say sometimes it's inadequate. But we teed it up in a way so that they could now put that spotlight on it, and he's given them the timetable.

Chairman LEVIN. Thank you.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

I'm going to pick up on two things you mentioned, and the first one I'll be criticized for as not politically correct. But I'll make this statement. If you're around Washington and you're in these hearings, it's one thing. But when you go back to Oklahoma, as I do every week, it's another thing. I'm always hit up with this idea, because not only—we're talking about the Fort Hood thing now, but I could talk to you about Abdul Mutallab, the Christmas bomber. The extremist views were evident from the University College through London, and it goes on and on. The November 19, 2009, the father reports and we all know about that report. Late November, he was added to the U.S. 550-name Terrorist Identities Datamart Environment (TIDE) and all this stuff.

All this stuff is stuff that we knew. That's not in your purview, I understand that. But nonetheless, it's the same. A terrorist is a terrorist. That's what they do for a living: They kill people.

I for one—I know it's not politically correct to say—I believe in racial and ethnic profiling. I think if you're looking at people getting on an airplane and you have X amount of resources to get into it, you need to get at the targets, not my wife. I just think it's something that should be looked into.

The statement that's been made is probably 90 percent true, with some exceptions like the Murrah Federal Office Building in my State of Oklahoma. Those people, they were not Muslims, they were not Middle Easterners. But when you hear that not all Middle Easterners or Muslims between the ages of 20 and 35 are terrorists, but all terrorists are Muslims or Middle Easterners between the ages of 20 and 35, that's by and large true.

I think that some time we're going to have to really—at least I'm going to have to have a better answer than I give the people back home, when people board planes or get into environments such as the environment that we're dealing with with this report.

I guess nothing more needs to be said from you guys on this. Let me first of all say, which I should have said first, there are no two people I think are more qualified to do the job that you have had to do than the two of you. You've been good friends of mine for a long period of time.

Now, something we can talk about, I think, a little more, a little easier. Your purview was really domestic, wasn't it? The continental United States (CONUS) was most of what you were talking about, was making the recommendations coming from what hap-

pened in the incident at Fort Hood. Did you look into outside the United States (OCONUS)? We have thousands and thousands of troops all over the world, and to me the threat is probably a little bit greater there than it would be here.

What thoughts do you have on that, or maybe recommendations you could have on that, to expand what you're doing to include that?

Admiral CLARK. We certainly did, Senator. The first thing that comes to mind is, every base where we exist overseas, we have non-Americans working with us on the base. What are the processes and the procedures for vetting these people? So we challenge it. We have a section in the report that talks about security clearances and how people gain access.

The second thing I talked about—identifying people who could become a threat, one of the things we have to look at is how we vet people in the OCONUS environment. I would suggest to you—and frankly, this would probably be better, the details of this we might talk about in closed session. But I would suggest to you that it was our conviction, and we would not have put it in the report if we didn't think that this was certainly a potential weakness.

Mr. WEST. Might I add this, Senator. If we take the lesson of Fort Hood—and admittedly, we will talk more specifically when you have your closed session—we have to be reminded that the thesis on which we're dealing here is essentially, for this whole report, the threat from within: the member of the military family who then turns against his or her fellow soldier, airman, sailor, marine, or coastguardsman.

The difficulty there, whether it is OCONUS or CONUS, is that with the universal access card, the ID, they can enter what should be the safest place either here or there, the base, the post, freely. With our automated systems now, we don't stop them for routine checks. So we can't—or we can. Certainly one of the lessons learned at Fort Hood was that they have now instituted some roving checks even of those who have the credentials.

But the place to stop them, the insider who's the threat, is not at the gate. It is to identify him or her before they can get onto the post and do that act. That's why all those signs that we talk about, all the cues and behavioral indications, even the ones that the chairman mentioned, are important for us to reemphasize, to expand and to focus on, to make sure commanders have that information. That applies both here and overseas.

Senator INHOFE. One of the things that was discussed here by the chairman was when can we move this along faster. I think you want to do that. We want to do that. We still have some of the recommendations of the 9/11 Commission that are not fully implemented and understood. So I would assume that you share those feelings.

I was down at Fort Hood about 3 weeks before this incident. That was when we had two of our Oklahoma units that were deploying overseas and I was down there for that event. Then I went down afterwards for the event that took place after the tragedy.

You had said—and I asked my staff to hand it to me so I could read it again. This is pretty remarkable, Mr. Secretary, when you said 2 minutes and 40 seconds after the initial 9-1-1 call, installa-

tion first responders arrived on the scene. One and a half minutes later, the assailant was incapacitated. Two ambulances and incident command vehicles from the base were there 2 minutes and 50 seconds later. I mean, that's really moving.

I would recommend, and maybe you've already done this, that you find out—not always looking at what is wrong, but learn from what was done right. In this case, I think it would probably serve us well to see how they did that remarkable job. I wanted to see it in writing after you'd said it, because I think that's remarkable. So I'd recommend you do that.

Mr. WEST. It was remarkable, and we did think that one of our jobs was to find out if that was the result of good planning, courageous and fast action, was there an element of luck, and, if it was what we believed and what we've said, excellent planning and well executed, is there a lesson to pass across the force.

One other thing I would add. I don't want to overdo—let me add it anyway. We tried as best we could to figure out what that meant, the passage of time from the first shot by the assailant to his last. That is, the whole event, because the uncertain part was how quickly the 9-1-1 call got in after the first shot was fired. The best we can make is that the whole shooting incident was ended by security forces between 7 and 8 minutes after it started.

Senator INHOFE. Were you surprised at that too, Admiral?

Admiral CLARK. I certainly was. This kind of a panel is supposed to find the things that are wrong. That's what we're supposed to do. But if you notice, we lead with some very strong statements about what we thought was right, because we wanted it up front that the people at Fort Hood did a fabulous job.

I testified yesterday and the staff reminded me that I said “fabulous” or “excellent” or “outstanding” 19 times yesterday. But I want to drive the point home. I said this was the best lessons-learned I've ever seen, and the performance of the people was brilliant. Were there things that could have been better? Yes. One of the reasons that it was brilliant was because of the brilliance of our people. They are so good.

Of course, nobody had the stopwatch going on inside the room where he was shooting, so that's why we don't know the exact time, as the Secretary indicated, between the first shot and the 9-1-1 call. But here's what we do know: There were a lot more rounds available, and they took that shooter down and the CID agent was handcuffed to him in a matter of moments and was with him from that point on.

Senator INHOFE. Let me commend all of them for the fine work they did.

Admiral CLARK. It was incredible.

Senator INHOFE. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Inhofe.

I would take 2 seconds just to say that I disagree with your comments about Middle Easterners and Muslims and the implications of those comments. I wouldn't want to say that except while you're here.

Senator INHOFE. Sure. I understand that. I expected that.

Chairman LEVIN. Thank you.

Senator Reed.

Senator REED. Thank you, Mr. Chairman.

Admiral Clark, you mentioned in terms of the threat a generic self-radicalization that would lead to violence. There are several different, as you suggest, categories of this, not simply Islamic radicals, but a host of others. Is there a strategy in DOD to identify these potential categories and to essentially work explicitly against them or to at least be aware of them?

Admiral CLARK. The first point, there are people in the public domain that have said we didn't use the magic term, "radical Islamics." We didn't do it on purpose. It wasn't because we were trying to be politically correct. It was because our task was to deal with violence and this was one of them. But I don't know how people could read our comments about self-radicalization and not understand that this kind of radical Islamic behavior is part of that group.

We said specifically though, the indicators are inadequate. Now, having said that, on Friday the Army published the list of 10, and having something out there is better than nothing. In the closed session, I would like to get into this in some detail.

But to say we believe that all of the indicators related to violence are not static indicators. We're living in such a rapidly changing world, potentially we should be considering the establishment of a group that focuses on this full-time. I have this whole series of kinds of behaviors that we are talking about—criminal, drug, domestic abuse, gang activity, supremacist ideology, terrorism, school violence, sex crimes, sabotage, arson, cyber. We're talking about all of these.

So I trust that's responsive to your question.

Senator REED. It is.

Mr. Secretary, do you have any comments?

Mr. WEST. There is an annex to our report that discusses the sources of violence in some detail. It's an example of the pieces that our researchers consulted. I think it's very informative and I commend it for reading.

I think that I agree with the Admiral's response. Also, in our executive summary, five or six key things that we recommend to the Secretary that we pull out from this report is the suggestion of a body that will collect the indicators of violence, update them in light of current circumstances, events in our world, occurrences in our world, and then make them available on an updated basis to the commanders and the supervisors who need to use them to make their judgments.

Senator REED. Let me again turn to the Admiral. Did you believe or conclude that there was adequate information coming from Walter Reed to Fort Hood with respect to the Major? Was there a problem there in terms of letters of reprimand that might have been issued or informal reprimands that were never fully communicated, so that the commanders at Fort Hood clearly weren't able to gauge the seriousness of this individual?

Mr. WEST. Senator, I wonder if you would let us discuss that with you in the restricted session. It's in the annex.

Senator REED. I appreciate that.

There's another issue and this, I think, can be—I'll let you decide—discussed in public, is that, there are many indicators about

Major Hassan's professional skills, far removed from his religious beliefs and his discussions, just simple competence, his ability to work with others, those things that are fundamental to being an officer in the military. Yet he was moved along. I know this question has come up. In these critical areas where there are not a surplus of individuals, such as mental health professionals, psychiatrists, et cetera, is there a double standard in terms of, had he been a line officer, an infantry officer, artillery officer—forget his radicalization, but just his simple performance, would that have gotten him kicked out?

Mr. WEST. I think again, Senator, we are prepared to discuss that with you, but we would ask you to let us do it in the restricted session.

Senator REED. I appreciate that.

Admiral CLARK. I would say certainly the heart of what we have to say is in the annex. Let me make a comment. We use the term "officership" in the open report. "Officership" was intended to mean more than just leadership, and it was our view that there were officership deficiencies. In the closed session we can talk in great detail about the specifics of that.

Senator REED. Just one final question—

Mr. WEST. If I might, Senator, I would just add also that in our one-page summary discussion, in chapter 1, in the open report, we do mention the findings and recommendations, which had to do with the Army's application of its policies to the perpetrator, but also the fact that there were signs that were missed and some that as far as we can tell were ignored. That's in the open part of the discussion.

Senator REED. Thank you, Mr. Secretary.

Again, part of this response is going to be training, not just commanders, but individual soldiers, sailors, airmen, and marines. We have something like that when it comes to a traditional threat, which is subversion and espionage, the old posters, World War II, "Loose Lips Sink Ships." That emphasis is persistent. Do you envision something like that in terms of the training elements going forward?

Admiral CLARK. I mentioned just briefly, but I probably didn't emphasize it well enough: There clearly has to be an outreach program here. I'm not talking about an outreach program outside the Department. I'm talking about inside the Department. Notice, the Secretary of Defense said on Friday—and we suggested that effective communication is the order of the day here. The Secretary started that process on Friday when he said to commanders: This isn't just ho-hum—I'm paraphrasing now—ho-hum, regular day-to-day stuff. Commanders should have to look past the day-to-day.

There is no doubt that a very effective training and outreach program is part of an effective solution.

Senator REED. Thank you very much, gentlemen.

Thank you.

Chairman LEVIN. Thank you, Senator Reed.

Senator Chambliss.

Senator CHAMBLISS. Thank you, Mr. Chairman.

Gentlemen, you have previously served our country well in your respective capacities and we appreciate your coming back once

again to help us deal with an issue that obviously is extremely important, at the same time extremely sensitive. So thank you for your continuing service.

In your report, you suggest that the Pentagon “coordinate with the FBI Behavioral Science Unit and the Military Violence Unit to identify the indicators specific to DOD personnel, and that DOD should use these indicators to develop an assessment tool for commanders, supervisors, and professional support service personnel to determine when individuals present risks for violent behavior.”

Now, my question is, don’t those tools already exist in the form of the Army Form 4856, which is the Army Developmental Counseling Form, and the Army Form 67–9, which is the Army officer evaluation report (OER)? Assuming these documents are used and filled out appropriately, shouldn’t we be able to identify a soldier who may be becoming self-radicalized as we think happened here and appropriately address the threat that they represent?

Mr. WEST. I’m going to let Admiral Clark have a good long swing at that because of his extensive experience with OERs and the like. But let me say what we were trying to do here, Senator. The fact is that there is a very good argument that there are tools out there that commanders can use to make the assessments they need to make. The question for us, though is, are there ways to strengthen what they can do and have we learned anything by the incident we faced and will discuss with you in closed session, from this incident, about how we can shore that up?

Frankly, things like OERs, there is a culture in the Services, all of them, which I think Admiral Clark can speak to better than I can, that doesn’t always find and report the kinds of things that would be better to report. For one reason, it may be because the information of some offense, of previous drug usage, but there has been a rehabilitation effort, or of some other contacts or signs, may have been left to the discretion of the commander as to whether to even keep that in the record so that it would be recorded in the OER. It never gets to the next commander, the next supervisor, and suddenly earlier signs are lost in the midst of the pass as they move forward.

We need to shore that up. We said to the Secretary in our executive summary, in our five or six big recommendations: You need to say to the officer corps of the Nation and all the Services that, what you report on these OERs and on things like the Service School Academic Evaluation Report (SAER), which takes the place of the OER when they’re in Service school, you need to say that that matters and that it has to be accurate and, most of all, complete, so that we can make the judgments we need to make.

Now, that’s the thrust of what we’re doing here. So, yes, reports exist, but they’re not being made use of in a way that fits what we need in these new and trying times.

Senator CHAMBLISS. So do you think it’s a matter of further education of those supervisors that are asking the questions and making that report?

Mr. WEST. I have an answer to that. It’s a question to me, but I want to get Admiral Clark involved. My answer is education, yes, but also making sure that the standards—and maybe that is edu-

cation—are applied. But there are also some recommendations for some further adjustments.

Senator CHAMBLISS. Admiral Clark?

Admiral CLARK. I don't know the first form that you referenced. I have the second forms here in front of me, so I can talk specifically to those.

Senator CHAMBLISS. The 4856 is the Army Developmental Counseling Form, which I understand is completed once a quarter. The 67-9 is an annual report for enlisted and officer personnel.

Admiral CLARK. I don't have that in front of me. But I would say that that form and the tools that go with that would be great if the person knows what the indicators are. Our review suggests that in the area of self-radicalization that can be very fuzzy.

The reason we suggested the FBI is they've already started doing some work here. So we're saying to the Secretary, don't start from scratch. But also the recommendation to use every expert that we know how to get, because we're looking for behavioral cues and their subtleties. Once those are known, I have every confidence that our leadership, our supervisors, will know how to deal with that.

But my interpretation of that was, we were talking about an education and that's why you have to have an outreach program that gets the training to the right people, so they have understanding of these issues.

Senator CHAMBLISS. If I'm hearing you right with regard to what both of you've said in your statement and your answers to the questions thus far, we did a great job responding at Fort Hood. Our men and women were courageous, heroic, and did a good job. But with the events leading up to the incident, we have some major deficiencies.

In fact, Admiral, you alluded to this, I think you called it "an evolving threat," were your exact words that you said earlier. Are there any protections or punitive measures that are in place to detect, for example, an individual who is one of those folks that I would categorize as an evolving threat, who might simply join a branch of the military with the intention of duplicating what happened at Fort Hood? What have we got in place now or what do we need to do to ensure that we don't have somebody who has spent the last 6 months in Yemen or 4 years ago spent 6 months in Yemen with the idea of ultimately coming back and having been trained to go in and duplicate this event?

Mr. WEST. Or who even spent a bunch of years or a month out in the wilds of our country becoming radicalized in a different way and under different pressures. The question is the same.

You're right, Senator, there was no failing by those at Fort Hood in their response. If there were gaps, it was in us as we tried to prepare ourselves to identify those factors that would say this person is going to be a problem, we need to act.

But I think your question was to the Admiral.

Admiral CLARK. I agree completely with what Secretary West has said. The thrust of your question gets us to this issue of the identification question that I raised this point to. That identification question raises things about the manner in which we do checks and what's involved there. I think it would be smart not to

inform an enemy in a public way about my particular impressions, and if it's all right with you that we talk about that in a closed session. But affirming your comment, this is part of the challenge. By the way, should we not expect that they're going to use every technique and scheme or maneuver that they can figure out?

Senator CHAMBLISS. Absolutely. That's why we have to, number one, get the information. But further, to your point you stated earlier, Admiral, is we have to share that information. It has to get in the hands of the people who are filling out those forms or who are making recommendations relative to an individual.

Thank you, Mr. Chairman.

Admiral CLARK. Mr. Chairman, can I say, since you made that last point, I say one more time: Get rid of the barriers, inside and outside of the Department, the barriers to information flow. Thank you.

Mr. WEST. Mr. Chairman, I'm sorry to keep this going, but could I add one more thought to that?

Chairman LEVIN. Sure.

Mr. WEST. Here's another problem that your questions and Admiral Clark's response raise, Senator. That is this. Let's take religion. The reason we have numbers and records on the representation of people of various religions in our forces is because they self-identify. They say: This is my religion, I'm an Episcopalian, or what have you. What about those who, formulating a reason to hide their purposes, don't disclose their religion, don't disclose anything that will cause us to try to—this is not your term—to try to profile?

It's the indicators, the behavioral cues, that we have to rely on. They are our only way of getting at this in any organized and aggressive and effective way.

Admiral CLARK. One more comment, then. So that you know, the alleged perpetrator was initially in the Army as an enlisted person and he went off and went to school. When he came into the Army the first time, he professed to be a member of the Islamic faith. When he came in as an officer, he did not declare. So all of the indicators aren't right in front of our nose. But I have all the statistics here to talk about every brand of religion that we know about.

The reality is that way over half of our people never ever declare what—they choose not to declare. So it's not always immediately apparent. That's why this is a challenge. But then really focusing on the behaviors, and that's what we wanted to put the spotlight on. The Department in its guidance and instruction to the commanders and all the people in the field are going to go by this document, and this document doesn't have sufficient guidance about self-radicalization.

Chairman LEVIN. Thank you very much.

Senator Ben Nelson.

Senator BEN NELSON. Thank you, Mr. Chairman, and thank both of you for your dedication and time in putting together a very well-organized and, I think, insightful report. We appreciate it very much.

So far we haven't really talked about, let's say, patient—or the evaluation process. Of course, connecting the dots requires that kind of an evaluation capability for it to be able to tell us anything.

In determining behavior, if you don't have all the background perhaps you can't establish that.

Violence in the workplace is not unique now to the military. It's part of everyday life, unfortunately, and that kind of violence isn't necessarily the result of self-radicalization in the workforce. So I'm wondering, in connecting the dots, as you look for not only self-radicalization, do you look for other indicators in your report? Shouldn't the military look for others, such as marital difficulties and other areas that, Admiral Clark, you identified in addition? Because self-radicalization is a subset of an overall problem when we talk about workforce violence, it may be that the military is unique in that respect because it's not just about domestic; we also have to face it on our military posts around the world.

So in connecting the dots, I think we understand that not all radicals will be engaging in violence and not everyone with a different idea will engage in violence. So what are other things that can be looked at in performance evaluations that would help us detect potential violence coming, not just from self-radicalization, but from others as well?

Admiral CLARK. It's a really great question and it drives us back to the guidance that's there today. We find that there are good indicators in a lot of areas. I mentioned a number of these. It includes the two that you talked about, although our view is that the whole workplace side is—we tend to focus on the kind of violence that takes place away from the workplace, not in the workplace, and that's a criticism.

But let's just talk about the domestic piece, for example. Earlier we talked about the requirement for balance. We have been dealing with this now for years. So we learned a long time ago that if the balance is incorrect we were going to have difficulty, because a domestic violence situation always has a "she says, he says" scenario ongoing. So we know how to do these things when we identify the behaviors.

So you're correct, we have them. We have the tools——

Senator BEN NELSON. We have the tools, right.

Admiral CLARK. This is why we're suggesting that perhaps we want to consider the establishment of an organization, a piece of the structure, that does this for a living, because you or I cannot define a solution set today and everything be perfect for the next 3 years. It's going to change.

Our suggestion is we need to understand the evolving world that we're facing. Let us not get sidetracked on just one little piece of this. The Secretary's goal was to make the workplace a safe environment. Imagine—and Secretary West really alluded to this, when the alleged perpetrator—he was an officer in the military, he was a field-grade officer. This implies trust. He's a medical doctor, implies more trust. He's somebody that a person would confide in. We can't have these kinds of people turning from the inside on our people and destroying the fabric of the institution and what we're all about.

So we are convinced that this then calls for the kind of investment that will ensure that we're staying up with the adaptation problem. This is a challenge, to be adaptive. I'm so pleased that the

Secretary of Defense addressed it straight-up on Friday and said we have to create a more adaptive force.

Senator BEN NELSON. Secretary West?

Mr. WEST. Just as an add-on, in terms of your question, what are some of the things that should be indicators, we have a whole list of recommendations. Incidentally, in our appendix C for purposes of being helpful to you we list all the recommendations, the findings and recommendations, and something about them, so that it's easier for you to find them without having to go all through.

At about 2.6 or so and all the way through that to 2.10 or so, there's a list of things that addresses what you said. For example, you said what about medical? Well, so did we. We know that the medical indications and medical records are protected, and they should be. But we raise the question of whether we shouldn't review whether there are ways to make some of that history, especially when it pertains to some things I've said before—drug abuse and the like—available on a more regular basis to those who need to have these indicators.

Senator BEN NELSON. If you don't have all the dots, you can't connect them.

Mr. WEST. Exactly.

Senator BEN NELSON. Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Nelson.

Senator Thune.

Senator THUNE. Thank you, Mr. Chairman, and I do want to express my appreciation to you, Mr. Secretary and Admiral, for all your service to this country, and obviously being called back into service for your extraordinary work in regard to this tragic incident.

I also want to take this opportunity to express my condolences to those who lost family members and loved ones during this terrible event. It was a horrific event in our Nation's history and the fact that it happened at Fort Hood, a place where more people have deployed to fight against terrorism than any other place, is really heartbreaking. Our heartfelt appreciation goes to those first responders who, once informed of the situation, as you have noted, not only arrived quickly, but showed tremendous professionalism and dedication to duty and in doing so saved a lot of lives.

I want to ask you about a couple of findings in your report. One is finding 3.8 of your review, which states: "DOD does not have a policy governing privately-owned weapons." Your recommendation states that: "DOD needs to review the need for such a policy." I guess my question is, can you explain what you mean by a privately owned weapons policy?

Mr. WEST. There exists, for example at Fort Hood, which among other things is a popular place for hunting, so a lot of folks come on to hunt—so the effort to have some sort of control over guns has to be carefully balanced, the need to come on and use it, but also the security of the post. The way that works and often works at a number of installations is this. First of all, all weapons issued by the U.S. military to its personnel are locked in the armory if you're enlisted or officer or what have you. They're secured. So on the day of the event, the only armed person on the scene until those who were part of the security force arrived was the perpetrator.

The policy works this way there. If you live in the barracks, then your privately owned weapon must of course be owned—properly registered in accordance with State and Federal law and the like, but also need to be registered with the commander so that they know what's there. If you live in the barracks, it is also secured in the armory. If you live in personal quarters on the base, properly registered with the commander, you keep them in your home. If you live off the base, the only requirement is that they be registered in accordance with State and Federal law, because you don't have them on the base. If you bring them onto the base, previously there was no way to know when that happened if you were a card-carrying member of the Armed Forces, if you had your credentials.

Now there's going to be a requirement, and I guess there always was—to the same rules as anyone bringing privately-owned weapons onto base: Let us know that you're bringing them on, right there at the gate.

What doesn't exist is any way in which bringing them on and concealing them, if you were a credentialed member of the Armed Forces, could have been detected. We really don't have the answer on how to deal with that, but we do know that it is a gap in the protection that was accorded to those that day.

We know one other thing. The policies vary from post to post. So the question we raised is simply this: Give some thought, DOD, as to whether you wish to have a DOD-wide policy with respect to the bringing and the use of private weapons on the post by those who are members of the U.S. military. Fairly straightforward.

Senator THUNE. You don't prescribe that. What you've just described is the policy at Fort Hood.

Mr. WEST. Right. It varies from post to post.

Senator THUNE. It varies from installation to installation, and the suggestion is simply that DOD adopt some uniform——

Mr. WEST. Consider, consider.

Senator THUNE. Okay. All right, without getting into the details of that.

That brings me to another question, because you have described the timing of the incident. News reports have indicated that it lasted about 10 minutes. Your report said 2 minutes and 40 seconds after the initial 9-1-1 call installation first responders arrived, 1½ minutes later the assailant was incapacitated, which accounts for about 4 minutes and 10 seconds of the timeline, which as you said, is almost superhuman in terms of response time. It really is remarkable and a great credit to those who responded.

But could we assume then that there was a time period before they got there, if in fact—I think you said 7 or 8 minutes.

Mr. WEST. That was our best estimate, but for the very reasons you pointed out, we're not so sure. We just stated the best estimate.

Senator THUNE. Okay. Which is still a significant amount of time; I guess the question is a follow-up to the previous question. But if the soldiers would have been armed at the time, in other words allowed to carry small firearms, in your opinion could more lives have been saved?

Mr. WEST. Might as well give an answer——

Admiral CLARK. Well, they're soldiers. If they had been carrying their weapons around on them, it would have been different. How different? How can I tell you? What would the timeline have been? But of course it would have been different.

Mr. WEST. What I was hesitating about is that I thought this was a natural lead-in to the active shooter program as well, which Admiral Clark spent some time talking about. Maybe we didn't go into it in detail, but the answer to your question is armed servicemembers could probably have done so. The difference, of course, is security personnel trained to take down someone in those circumstances differently, and in two ways.

In the past the practice has been clear out all the innocents, those who are unarmed, those who are being assailed, and then you take down the shooter. That has been the practice for law enforcement agencies throughout the United States as well. But there has been the advocacy of the response to active shooter program, which is more and more becoming the response, which is: Train your security people with firearms and then go in, and as your first priority, take down the shooter before he or she can do more damage to those who are there.

But the risks are obvious and that's why the emphasis is on training. The FBI, who are the experts on this, have cautioned that you really need a carefully selected and well-trained force to do that. It was done at Fort Hood.

Senator THUNE. They performed extremely well.

Admiral CLARK. May I add one other point? My response was brief, almost to the point of being brusque, let me just add. It would have made a difference, but if I were a commander would that be the first thing that I did, arm all the people on the base? That's not what I would do. Would it make a difference if some portion of them were armed? Of course it would. But the reason I wouldn't just summarily arm everybody is because of the fact that it would so change the environment that we live in. I don't think that's the immediate solution to good order and discipline.

Senator THUNE. I guess in response to that, if, in fact, there is going to be some consideration given to a policy, a Department-wide policy with regard to firearms, I would hope it would not be more restrictive, because I do think these are soldiers. These are people who are trained. Clearly, if anybody would be prepared, probably not trained exactly in emergency response, but people who would be trained and prepared and equipped to effectively use a firearm to save other lives, it would be someone in the U.S. military. That's my observation.

So I have some other questions, but I'm out of time. So thank you all very much.

Chairman LEVIN. Thank you, Senator Thune.

Senator Burris.

Senator BURRIS. Thank you, Mr. Chairman. Mr. Chairman, may I go on record as also objecting to the comment that was made by the distinguished Senator from Oklahoma in reference to profiling.

I also want to commend the two distinguished public servants here, one of whom I've known since he was a freshman at Howard University, and to see him move through the ranks and commit all of this service to America is what I anticipated when I saw him as

a freshman when I was in law school at Howard, and then of course seeing him graduate also from Howard Law School. So, Secretary West, you have done a tremendous job for the people of America and we are very, very grateful to you for that.

Mr. WEST. Thank you, Senator. Your own lifelong record of public service is quite distinguished and I consider your compliment that much more valuable. Thank you.

Senator BURRIS. Admiral, I appreciate your service as well. I just didn't attend school with you.

I am really seeking to see how we get at the major problem that you were tasked to do. I had other questions, but the hearing has just provoked some other thoughts. Mr. Secretary, you mentioned the fact that when you take an oath of office in the military—and I'm just wondering whether or not there's a different standard under the constitutional rights that you have after you've taken the oath of office. It's something I may have been missing because I've never been in the military, and I just want to know whether or not a person who has taken an oath, there are different standards that they are held to, for example, the free speech article or the right to bear arms article, which was brought up by Senator Thune. Could you comment on that, please?

Mr. WEST. I will, and then I think you'll be interested to hear the views of someone who has commanded at every level and has had to give these instructions to his officers and those serving under him.

Years ago I was the DOD General Counsel, so we tried to remain conversant with this for obvious reasons. I was a Judge Advocate General officer as well. The basic rule is stated: Servicemembers, whether they are officers or enlisted, who come into the Services are still citizens of the United States. They do not give up their basic constitutional rights and protections. They get to speak, especially when they're on their own time and not in uniform, freely. They get to associate under the same circumstances. They are entitled, if they are accused of criminal activity while on Active Duty, to a trial with a number of the constitutional protections, not all, because, as I think Admiral Clark observed, they do agree when they take the oath of office to put some things, as he said, on the shelf. For example, when they're in uniform they can't just say anything they darn well please.

I may have said it too broadly. There are lots of things you can add in, qualifications. But it's just a fact of life and, frankly, when they're on Active Duty in uniform they can't just go anywhere at any time to do whatever they please. They are under orders. They are under obligations, either as officers or as noncommissioned officers, to respond as they are directed, to carry out their orders fully. They represent this country as well as serving it.

Now, I've said that way too broadly, I'm sure. But I think it gives an overlay. It says yes, they don't ever stop being citizens, they don't lose their constitutional protections, but there are some limits that can be imposed on them under lawful military authority.

Admiral CLARK. Secretary West said all of that like the true veteran that he is. It was absolutely perfect. I would just add that, so let's say we're having a time—it's the political season and people are running for office. A member of the Armed Forces is not al-

lowed to show up there in uniform. Now, if they choose to do so—and I'll use my words very carefully—they will be counseled, to be sure. I would say they'll probably be part of a short but exciting conversation, is the way I might put it.

There are other areas. When we're overseas, the first thing we tell our sailors is: Remember, you are ambassadors of the United States of America. We put limits on the kind of things that we expected them to do and things that we clearly expected them not to do. So those are the things that we are speaking to, and certainly, as Secretary West said so correctly, basic constitutional rights are never in question.

Senator BURRIS. Thank you, Admiral.

Another general question that's running through my mind. Now, in your work in this short period of time did you seek to assess other violent acts that may have taken place on military bases, on American soil or military bases, say the incident in Iraq where one of the soldiers supposedly snapped and killed fellow service persons? Did you look into any of that?

Admiral CLARK. Absolutely. Team one went into great detail of policies across the board. They're the group that reviewed over 30,000 pages of instructions and policies. It was incredible. We called this the omnibus team. It was an unbelievable task that they had. They used as a frame of reference to look into these special cases and say, now are there weaknesses here? Because the Secretary of Defense asked us to look for weaknesses in policies, programs, procedures, and gaps. So we looked at those, and basically we found that—this instruction, by the way, that I hold in front of me has extensive detail about the questions you raise about the things that you can and cannot do. In other words, the prohibited activities are outlined here.

But our team used those particular cases like you cited as a springboard and said, are the policies adequate? Fundamentally, what we're reporting is that—and let me inject this thought. We know that you can't legislate perfect behavior. That's not possible. So the question is, are the policies fundamentally sound? The areas that we have put a focus on in the report, specifically this internal threat is the area where we see the greatest need.

Senator BURRIS. I just wonder, gentlemen, whether or not in your assessment and in your report we're trying to get at something through procedures that is almost impossible to prevent. It's similar to a suicide bomber, as I would see it, a person who is willing to commit his own death. All the policies and procedures that we would put in place, all the corrections—for example, Mr. Secretary, if you were to have some type of procedure to go on base, whether or not you bring your private arms on base or not, what happens if the commanding officer was to have a problem? Do you think that the military police is going to stop a commanding officer at the gate and search him for his own private weapon and determine whether or not, if he's bringing that weapon on base, if he is determined to make some type of violent act or statement?

I just bring that up as a result of our attempt to try to get procedures that are going to be in the place that would seek to prevent someone from doing such a violent act.

Mr. WEST. That's a very pertinent observation, Senator Burris, and it is exactly on point. It is why we have emphasized in our report that we can't rely solely on stopping someone at the boundary. We have to have looked for the signs, for the 100-yard stare, for the examples of tensions or difficulties even in a personal life, and we can do this if they use government facilities—for the communications with extremist persons or organizations on a repeated basis.

We can look for all those signs. We can look for the signs of drug abuse because—and I mention that so often because there is some literature that our team one found, incidentally, has its report in chapter 2. We looked for those signs—that say that past drug abuse, even when corrected, is often linked to later outbreaks of violence. So we have to look for what Admiral Clark discussed in his opening statement as the behavioral cues and indicators, and we must do that over the course, say, of the colonel's service, to find them early enough so that it doesn't get to the point that he brings his weapon onto their base in some crazed effort.

Now that is the thrust, frankly, of the entire report, and thank you for getting right to the heart of it.

Senator BURRIS. Mr. Secretary, the question is, can this and will this happen again? God knows we don't want it to. But think about it.

Thank you, Mr. Chairman. My time is up.

Chairman LEVIN. Thank you, Senator Burris.

Senator LeMieux.

Senator LEMIEUX. Thank you, Mr. Chairman.

Secretary and Admiral, again to add to my colleagues, thank you for the work that you've done. Thank you for your past service. Thank you for this service.

I also want to extend my condolences to the families of the Fort Hood soldiers who were killed. We're keeping them in our thoughts and our prayers.

I want to, first of all, just state that I think we all agree, and your report certainly says, that this was a failure on the front end. We commend the first responders for their fantastic work, but this was a failure. I don't want to belabor that, because I think it's been talked about, Mr. Chairman.

But there's a Houston Chronicle article of yesterday, Richard Lardner and Calvin Woodward, that I'd ask be submitted for the record, which I think details a lot of the failures in monitoring Major Hassan along the way, and that something should have been done to prevent this.

Chairman LEVIN. It will be made part of the record.

[The information referred to follows:]

Houston Chronicle  
January 20, 2010

## Troubles Seen At Every Turn In Hasan's Medical Training

By Richard Lardner and Calvin Woodward, Associated Press

WASHINGTON — Often teetering on failure during his medical training, Nidal Hasan hit a particularly rough patch in 2007 when his Army superior cited him for unprofessional behavior, inappropriately discussing religion, underperforming in his residency program and being too fat.

Yet the same supervisor who meticulously catalogued Hasan's problems suddenly swept them under the rug when graduation arrived that year for the man now charged in the Nov. 5 massacre at Fort Hood, Texas, government documents show.

Hasan, then a captain, was rated "Outstanding Performance, Must Promote" by that supervisor, Maj. Scott Moran, and as "Best Qualified" by another, Col. John Bradley, shortly after he barely escaped the punishment of administrative probation.

Reached by telephone, Moran declined to comment. Calls to Bradley's office were not returned.

And in direct contradiction with the record about the psychiatrist in training, Moran reported after Hasan's graduation that there was no documented evidence of unprofessional behavior or other problems in his academic past.

Defense Secretary Robert Gates last week released an internal Pentagon review that found several unidentified medical officers failed to use "appropriate judgment and standards of officership" when reviewing Hasan's performance as a student, internist and psychiatric resident.

Gates withheld details, noting that the findings had been referred to Army Secretary John McHugh for possible disciplinary action against the officers.

But the disjointed picture emerges through information gathered during the internal review and obtained by The Associated Press.

The information reveals a pattern of sanitized performance appraisals — praise piled into the official record by officers who seemed determined to advance Hasan's career despite knowing he was chronically late for work, saw few patients, disappeared when he was on call and confronted those around him with his Islamic views.

The material exposes concerns about Hasan at almost every stage of his more than decade-long Army education.

Senator LEMIEUX. Thank you, sir.

What I want to talk about is three things, and there are questions for you. The first one is to follow up on what Senator Thune was talking about concerning soldiers on the base carrying weapons. This struck me as well because I recently this past week went to four military bases in Florida, from Naval Air Station Pensacola, to Tindall, to Eglin, to Hurlbert Air Force Base. The thing that you notice different than going to a military base in a theater of war, like going to Bagram Air Force Base, is that the soldiers and the airmen and the sailors aren't carrying weapons. But when you're at Bagram you see half of the service men and women carrying their weapons.

I don't think that this would have happened potentially at Bagram Air Force Base for two reasons. One is there would have been a huge deterrent to Major Hassan if he knew that the other soldiers were carrying weapons. The second thing is, if it would have happened, to follow up on Senator Thune's point, that 4 minutes of time or whatever the period was where there was no first responder there, one of our servicemembers I am sure would have picked up their weapon and fired back.

I hope that you will in your continuing work stress this to the Secretary of Defense, because, while I understand the Admiral's point about order on the base, there is probably a sweet spot here where some of the folks on a base, even in the United States of America, should be carrying weapons, maybe where there's going to be large groups gathered, I guess like where this processing center was happening.

So I don't know if you have any further comments on that. You've already answered Senator Thune's question, but I want to make that point. Mr. Secretary?

Mr. WEST. I have a comment, and that is this. It has happened overseas where people have been carrying weapons. We've had incidents in which a soldier has gone berserk and started shooting and there were weapons around him; it didn't stop it.

Second, let's assume that everyone's able to carry weapons, say at Fort Hood. Well then, for a committed person it wouldn't have been necessary to smuggle them in to use them.

Then third, I guess—well, no. I think first and second is enough. If the Admiral wants to add a third, I will let him.

Admiral CLARK. I don't argue with your fundamental point. I would just say that as a commander I realized that I was responsible for the creation of the environment. So the deployed environment is always different than the environment at home. So I think there are a lot of things that I could figure out how to do before I decided to arm every single human being on the base.

I don't discount at all your point about the degree of difficulty for a shooter. But I believe Secretary West has accurately responded. We have cases, to be sure, and we have been very careful not to define specific single-point dot solutions for these cases because, for starters, we did this in an extraordinarily short period of time. If we were going to then look at all the possible courses of alternative solutions for every one of the recommendations we made, we would have needed at least 6 months and not the short time we had.

Senator LEMIEUX. I understand that. I'm just saying that there's a general point. I used the term "sweet spot" for a reason, not that you would put a gun on every service man or woman's side, but that there be some thought about this point, because I do think that knowing that someone is bearing arms is a deterrent. Maybe it hasn't always been a deterrent, but it can be a deterrent. It certainly might have saved 13 people. We don't know, but it might have saved some of them.

The second thing is, in terms of—Senator Collins is going to speak in a minute and her Homeland Security and Governmental Affairs Committee, along with Senator Lieberman, has talked about the need for training for all servicemembers in identifying signs of Islamic extremism. I wonder if we don't only need to en-

courage our servicemembers to look for these signs and report them, but that we need to do more than that and require it.

I think about something that universities do. I didn't attend the University of Virginia, but I understand they have a very stringent honor code. The honor code can be broken in two ways: one, by violating it; and the second is failing to report that someone else violated it. I wonder for your consideration, whether or not we should make a suggestion like that, that you have an obligation as a member of the U.S. military that if you see something that is out of line, to report it. There, if I feel like in my service record I'm going to be reprimanded for not reporting something—none of us like to tell on our colleagues. It's human nature. But I also commend that to you as something you could consider, and if you want to comment on that I'd appreciate that as well.

Admiral CLARK. I think these are the kind of questions, all in pursuit of potential solutions, that the Secretary would think is going on, without suggesting whether one is the right solution or not. Phase two is to do the drill-down, and they couldn't do the drill-down on the whole breadth of things that we looked at 30,000-plus pages of directions and policies and all of that. Our job was to put the spotlight on the key things that they could go do in a hurry. It's my understanding that's his expectation for phase two.

Senator LEMIEUX. The third and final point I have is, we've heard this phrase, "connect-the-dots." I heard it yesterday when we had a Commerce, Science, and Transportation Committee hearing with Secretary Napolitano and Director Leitner about the Christmas Day bombing attempt. That's, obviously, the great struggle, is connecting the dots. You mentioned, Admiral, perhaps having some other special unit or division of people who would try to do that.

That seems to be smart to me, that you have someone who's going to look through all of the information, not be tasked with maybe other jobs, but be tasked with trying to—I don't know if it's an internal affairs function or if it's just a function to make sure that someone is out there looking at these reports that are filled out on different service men and women. I know there's a lot of people in the U.S. military.

But we have really good technology in this country, technology that's being used by the private sector. I don't know if these reports are scanned. I don't know if they're entered on a computer. I don't know if someone can use cloud computing and some of these new techniques to do searches.

We've failed again on the almost terrible tragedy on Christmas Day because of a misspelling of a name and other things that failed in our intelligence and the way that we process, gather, and evaluate intelligence. One thing I just might commend to you in your further discussions with the Secretary is, if you do establish one of these units, talking to people in the private sector who develop this wonderful technology and see if it might be an aid for helping keep our service men and women safe.

Admiral CLARK. May I comment? We say in the report that we've been having arguments about who owns what pieces of information. We've been having those discussions long enough. It's time to move on. So without defining what that solution is, I don't know

how a commander can possibly connect the dots if he doesn't have all the dots in his dot kit. "Dot kit" may be the right term.

But also, I bring attention to this point. We told the Secretary this isn't just interagency. This is inside the Department as well. Challenge the assumptions on who has all of the pieces of information. The commanders will be better equipped and we know how brilliant they are when they're given the tools.

Mr. WEST. Actually, I think the organization that you're thinking about that we recommended was one that's designed to collect all the indicators, keep them catalogued, update them regularly, and make them available to commanders and those who have to make decisions. Your idea has, I think, to do with connecting dots on specific individuals, where those things come up. That's an interesting concept and it's not one that we necessarily focused on. Thank you for that.

Senator LEMIEUX. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator LeMieux.

Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman. Thanks very much to Secretary West and Admiral Clark for the service that you've given in doing this report, and of course throughout your lives. The attack of November 5, 2009, was a tragedy and we're very grateful for the efforts that you've made along with DOD personnel working with you in this review to ensure that such a tragedy doesn't happen again.

The Homeland Security and Governmental Affairs Committee—and Senator Collins and I are here—has been investigating the Fort Hood shootings to assess the information the government had prior to the shootings and the actions it took in response to that information. I can tell you that, even at this early stage of our investigation, it's become apparent to us that DOD's approach to the threat of servicemembers who adopt a violent Islamist extremist ideology needs to be revised.

Senator Collins and I sent a letter last week along those lines to Secretary Gates. I know there's sensitivity on this about the other Muslim Americans who are serving honorably in our military, but I honestly think that a more focused approach, an open approach on Islamist extremism, will protect the overwhelming majority of Muslim Americans serving in the military, who are serving honorably, and will maintain the bonds of trust that are so necessary in a military context among servicemembers of all religions.

It seems to me in the Fort Hood case that there were many indicators that Nidal Hassan was motivated to commit these murders in furtherance of his own violent Islamist extremist ideology. But I must say respectfully that your report only tangentially mentions that particular threat. In contrast, your review recommends generally that the Department "identify common indicators leading up to a wide range of destructive events, regardless of the individual's identity."

I understand again DOD's need to be sensitive to the religious beliefs of all its servicemembers and employees. But I think it's also critically important, and I don't see it in your report, as much as I admire so many of the recommendations you've made, that we

recognize the specific threats posed by violent Islamist extremism to our military.

So I wanted to ask you first, how do you think the Department and the Services should address the specific threat of violent Islamist extremism and if you want to respond to my concern generally about this? I will add that I remember being disappointed, troubled, after the Fort Hood murders when General Casey's first response described the incident as a force protection failure, which I suppose in one sense it was. But it was also a terrorist attack in my opinion. To a certain extent, the title of your report, "Protecting the Force," continues that emphasis, as opposed to a focused emphasis on the problem we're facing now, just as we focused earlier, after Fort Bragg, on the very real problem explicitly of white supremacist extremism.

So I welcome your response generally and particularly.

Mr. WEST. I was the Secretary of the Army at the time of the Fort Bragg, Senator, and because I was given a little more leeway I was the one who ordered the review that occurred. We operated under the same constraints then that—the folks we appointed operated under the same constraints then that we operate under now. That is, they had an ongoing military justice investigation and in fact, because the victims were civilians and the acts occurred off post in Fayetteville, still to this day one is struck. I mean, the servicemembers required two civilians to kneel and shot them execution-style.

So there were several, multiple criminal investigations, and so that task force that we appointed could not get into what might have been criminal aspects or anything that would have imperiled the trials. We operated under that same constraint.

Senator LIEBERMAN. Okay, so that's the reason you thought you couldn't be more explicit about Islamist extremism?

Mr. WEST. What we had to say, a lot of it is in the restricted annex. But no, I think to your second point we had is, respectfully, yes, it was and yes, it is a force protection issue. That is the way in which it was handed to us and that is the way in which we had to approach it.

In that case, it is every kind of extremism, every kind of opportunity for violence, that we, if we're going to have this one shot, Admiral Clark and I, to make recommendations to DOD, have to be sure to cover. So yes, we went for indicators, for cues and the like, but we did not exclude any source of violence and we specifically did not exclude the source that comes from radical Islamic belief associated with the actions that go with it.

Admiral Clark has some thoughts I know he wants to add. We talked about it more than once. So I'm going to stop here, but that's my brief oversight of how we approached it.

Senator LIEBERMAN. Let me just, before we go to Admiral Clark, just follow up while I'm thinking about it, because after those heinous murders at Fort Bragg in 1995 the Army, as General Keane testified to us, issued a pamphlet, training materials, that are quite directly oriented towards supremacist activities and other racial extremism, and specifically detailed some of the key indicators to look for in white supremacists, which I thought was exactly the right thing to do, of course.

I guess the question now is do you think the Services should issue a similar type of pamphlet with the same kinds of recommendations to address the threat of violent Islamist extremism, because that is the reality. Of course—do you want to respond to that?

Mr. WEST. Only that I think you make a good point.

Senator LIEBERMAN. Okay, thank you.

Admiral, please.

Admiral CLARK. Good to see you again, Senator.

Senator LIEBERMAN. You too, Admiral.

Admiral CLARK. In my opening statement I talked about violence and I made the point that some have indicated that we did not address the kind of violence that you're speaking to, radical Islamic fundamentalism and the behavior that goes with that. The point that I made is, yes, we did. Because Secretary Gates wrote us a set of terms of reference that talked about violence in the workplace and the people, including people hurting themselves, we decided to go after it in that way.

But we used the term "radicalization" and "self-radicalization" dozens of times in the report, which we intended to make clear we're talking about every kind of violent behavior, including this. Then we go on to then specify in our recommendations—and I made the point about, here's the DOD directive that talks about prohibited activities. Our point is this document is inadequate to the task when dealing with self-radicalized individuals.

So that's what we're talking about. I could not agree with you more completely that we need the outreach program. "Outreach," I mean we have to reach out and let people know what the positions are and where the red lines are in behaviors, and then with that goes all of the training that you talked to. So I made that a matter of my prior testimony and I'm in complete alignment with that view.

Senator LIEBERMAN. I appreciate that clarification. In my opinion, because—of course there's a concern about force protection generally. But because this is a unique new threat we're facing, I think the more explicit we are about it the clearer it's going to be and the better off we're going to be, because, as somebody said, some of the regulations earlier had to do with almost Cold War scenarios, and then the obvious response to the white supremacist killings. Now, unfortunately, we've had now two cases, Akbar in Kuwait and Hassan. Unfortunately, the way things are going, we'll probably have some more. So for the protection of the force, I think we have to be really explicit about what this threat is.

My time is up. Thank you.

Chairman LEVIN. Thank you very much, Senator Lieberman.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Gentlemen, it's good to see you both. Thank you for your continued public service.

Senator Lieberman, the chairman of our Homeland Security and Governmental Affairs Committee, has asked exactly the questions that I planned to ask, which is not a surprise because we've been working together on the whole issue of homegrown terrorism and the threat of Islamist extremism.

I do want to follow up a bit on the point that Senator Lieberman just made, because I was struck when I read the public part of your report by the decision to omit the term “Islamist extremism” from the public report, and it troubled me. It troubled me because it appeared to contrast sharply with the approach that DOD has taken in the past. Your report recommends that the Army focus on a broad range of motivations for violence rather than focusing on specific causes. But that’s not what the Department and the Army did after the racially motivated murders associated with Fort Bragg back in 1995. The 1995 guidance is striking because it squarely faces the problem, and I believe that’s why it was so effective. It sent a clear message that white supremacists had no place among our troops.

I believe we need to send a similarly clear message. Indeed, in 1996, in response to the Fort Bragg incident—and obviously, Mr. Secretary, you’re more familiar with it than I since you were involved in correcting the problem at the time—but in response, commanders were specifically advised to be aware of “indicators of possible extremist views, behaviors, or affiliations.” They were told to look for specific signs, such as reading materials or the use of a personal computer to visit extremist sites. These signs were geared toward identifying white supremacists within the ranks.

What Senator Lieberman and I have suggested in our letter to Secretary Gates is that same kind of focus, squarely admitting what the problem is. So my worry is that the perception of your report for those who only get to read the public part will be that we’re not facing the problem squarely the way we did in the mid-1990s, and it worked. The guidance was excellent. It involved training our commanders or enlisted troops, and it appears to have been very successful.

So, without presuming to speak for my chairman, Senator Lieberman, that’s what we’re suggesting, that we squarely face this threat to our troops.

So I would end what I realize has been more of a comment than a question by urging you to more explicitly address this specific threat. It doesn’t ignore the fact that there are other sources of violence. But in fact, family violence, suicide prevention, sexual assault, all extremely important priorities for us, but they are different in their nature than the threat from Islamic extremists.

So I’d ask you to comment particularly on whether we should have specific training to recognize the signs of radicalization in this area. Mr. Secretary and then Admiral Clark.

Mr. WEST. It’s almost impossible to have a comment, Senator. That was a very powerful statement, along with Senator Lieberman’s statement. You of course put me a little bit under the gun by pointing out that that’s what we did in the Army when that occurred.

I won’t even spend time on the distinctions. I think there are some clearly. Being a white supremacist carries no overtones of constitutional protections of any sort, whereas a religion is always—I know I’m going to be accused of being politically correct here, but so what—is always an area where we have to go carefully.

For example, religious extremism, violent, aggressive religious extremism, is a source of threat to our soldiers, sailors, marines,

airmen, and coastguardsmen, whatever the religious source. We need to be careful, and we tried to be careful when we did this, to make sure that we turn the military's attention inward, since the person that was quoted earlier as having talked about the Cold War, that was Secretary Gates. What he was pointing out was something we said, which is we have been focused on the external threat. Now we have to look at the internal threat, from within, from one of our own.

As I said before, this is our one shot at it, Admiral Clark and I, and we want to make sure that we look at the indicators, and religious extremism, whatever its source, is an indicator, and there are a whole bunch of things to look at. I think that description is right. The fact, as you both make it, that it is Islamic religious extremism, I think it is a point worth making. I think the Secretary and everyone will hear it and they will react accordingly. But that becomes part of the history of this discussion.

Senator COLLINS. Admiral Clark.

Admiral CLARK. It's so nice to see you again, Senator. It's been a privilege for me to be engaged working on this task. When the Secretary of Defense asked me to do this, I did so because I believed it was so important.

Let me say that within 5 minutes of it going public that I was going to co-chair this task force with Secretary West, my very good friend General Jack Keane was calling on the phone and telling me in great detail—I was driving down the road on my cell phone, and he was explaining to me how they did it. He happened to have been in command down there at Fort Bragg and I was commander of the Second Fleet and we were friends and worked together down there then.

So I've been mindful of his point of view on this since the very, very beginning and was in complete alignment with it.

To build upon my response to Senator Lieberman, I'm just going to give you Vern's view here. We talked about this a lot, how do we shape this. If we shape this as—if the report was full of reference to radical Islamic fundamentalist activity and behavior, some people would have read it that it was going to be all about that. The Secretary of Defense clearly gave us another task. He gave us the task to deal with violence in the workplace across the board, and because he did we made the decision that we were going to handle it the way we have presented it, but when questioned about—we frankly, Senator, didn't know how people were going to be able to misread the references to self-radicalization. We thought that that was going to be pretty clear, but maybe it wasn't clear enough.

Our focus then, and one of our primary recommendations is the guidance on these behaviors is inadequate, and the way you make it adequate is you decide what the red lines are going to be, you inform your people, you do everything that you know how to do—and that's called training—to ensure that our people know how to respond. That's what those of us who've had the privilege to command are charged to do. We talk about officership in the report and so forth. That's what leaders do and that is what is required.

Senator COLLINS. Thank you.

Chairman LEVIN. Thank you very much, Senator Collins.

I was listening to Senator Lieberman and Senator Collins with the suggestion that we address a specific threat, since it obviously is a specific threat. It is appropriate that our leaders be directed as to how to address that threat, just the way they were, I guess, in the 1990s with the white supremacists, but to make it clear and to make it certain that it's not viewed as an anti-Muslim effort, but rather an effort to address violent extremism, radical Islamic extremism, it would be very essential, it seems to me, wise that people who were involved in preparing that kind of instruction include Muslims, because obviously that would be important in terms of knowledge of the threat, but also important in terms of making it clear that is not anti-Muslim. 99 percent of Muslims are not people who are engaged in these kind of activities, and to make it clear it's not this kind of an effort, which I think is a legitimate effort, that Senator Lieberman and Senator Collins talk about. That is a legitimate effort to make it clear that it is not aimed at Muslims, but aimed at violent Islamic radical extremism, and it's important that Muslims be significantly involved in that direction.

I was wondering if Senator Lieberman or Senator Collins might want to comment on that suggestion.

Senator LIEBERMAN. Mr. Chairman, I think that's an excellent suggestion. In some ways you've given voice to it. But it would be a real omission, as I hear you talk, if it wasn't done, in other words if Muslims weren't involved.

One of the things in this fact situation that troubles me, and I suppose why I feel like we have to talk explicitly to one another about this threat, including most of all to have in the conversation Muslim Americans. Obviously, as Senator Levin said, 99 percent plus are not extremists or terrorists.

I worry as I look at this fact situation in Hassan's case that part of the reason that commanders and others who after the attacks at Fort Hood were spewing out to the media these signs that looked back and said he showed he was really turning in a very extremist, anti-American direction, that people didn't voice them or record them because of political correctness and, even more than political correctness, the sensitivity that we all have about religious discussions.

But the truth is, the best thing that could happen here, it's a great place for it to begin, in the military, is to have a real open discussion about this. Of course, for it to be a real discussion it has to include Muslim Americans. So I think your suggestion—in other words, I think that if Muslim Americans had been seeing—I don't know what the facts were about this—some of the things that Hassan was saying at Walter Reed, for instance, I think they would have been alarmed, because this doesn't reflect what they think.

Therefore, Mr. Chairman, I think your suggestion is really an excellent one. Thank you.

Senator COLLINS. Mr. Chairman, if I could just respond as well. I too think that your suggestion is an excellent one and it's very consistent with the approach that Senator Lieberman and I have advocated on the Homeland Security and Governmental Affairs Committee. In fact, in our letter to Secretary Gates where we suggest more training, we point out that updating the approach would help to protect from suspicion the thousands of Muslim Americans

who are serving honorably in the U.S. military and help to maintain the bonds of trust among servicemembers of all religions and enhance understanding.

So the steps that we have recommended would clearly benefit from the inclusion and active involvement of Muslim Americans, and that's what we intended. But I also think it has benefits for Muslim Americans serving, so that other servicemembers have a better understanding of Islam. So I'm in complete accord with what you suggest. I think that is along the lines of what we were proposing as well.

I would ask that we share with our two distinguished witnesses today the recommendations that Senator Lieberman and I have made in our January 13 letter to Secretary Gates, because as you go forward with your work it may be of value to you as well, we hope.

Chairman LEVIN. Thank you. One other thing that seems to me would be appropriate, and I don't know if you've addressed this, but it's sort of along this line: that our policies also should be very clear about why it is unacceptable, why it's not allowed, prohibited, to have taunting or harassment of people because of their religious views, as, according to the public record, occurred in the Hassan case.

I don't know if that's true and I can't comment on your annex, but it seems to me this is part and parcel. Religious tolerance does not mean tolerance for violence and extremism. It doesn't mean that, as I pointed out maybe an hour ago. That's not what we're tolerant of. But what we are tolerant of, and proud of it, is other people's religious views. As part of that, it has to be importantly pointed out in the military that that means we do not accept taunts, graffiti about "ragheads" or what have you, about anyone's religious views. I don't know if that is part of your recommendations here, that that be clear as well in terms of guidance, but it seems to me it's an important part of it.

Admiral CLARK. Let me address it. It's very well covered in the prohibited behaviors and activities.

Chairman LEVIN. You mean currently?

Admiral CLARK. Currently. It's very well spelled out. So I've spoken only to what's not in this document. What's in this document is 100 percent right, and what we have said in this document does not have the piece in it regarding self-radicalized behavior.

Mr. Chairman, I so want to appreciate the fact that you have collectively recognized the very effective and loyal service of thousands of Muslims. Somebody accused me of being politically correct. I don't care. The way you said it is exactly right and I appreciate it.

Chairman LEVIN. One thing to make this even more complex. When we talk about connecting the dots, and we have to do a far better job of connecting the dots—I believe that's the greatest failure in this and the other incidents that we've been discussing in various committees—there are counter-indicating dots that complicate the work, including with Major Hassan. It's not just those dots which in my view would have made folks suspicious, had they known about it, of what his potential was, but there are some dots that go in the other direction in terms of—and these are in the

public record—what his patients thought of him, which was very high. You have to throw those dots into the mix, too, for people who are going to be judging him.

You have a record here of a number of his assessments were not just negative—that should have been included in the record, by the way; I happen to agree with you totally—but there’s also some highly positive, not politically correct for that reason, but positive, assessments of his capability.

I just think it’s important that, since we’re trying to take a general view of this, that while it’s critically important to do a far better job of collecting dots, that we also recognize in terms of the task in front of us that there are some dots that are going to be in that mix which make it very unclear what you do with the dots which seem to point in one direction, because there are some dots that point in the other direction, even with him. They’ve not been focused on, obviously, but there are some counter-indicators here which are fairly clear as well.

Finally, Admiral, you talk about reducing—“eliminating” I think is your word—the barriers, get rid of the barriers to information flow. I think generally you’re right, and there’s barriers here which clearly should not be there. So I agree with your premise. Are there any barriers that you’d want to maintain, either privacy barriers or barriers—for instance, you talked about I think prior drug problem or an addiction problem which has been overcome. Some of that’s not passed along now. If it’s been overcome, I think there’s some instinct in commanders that maybe we should just let certain things not be passed along which would unfairly perhaps hurt somebody’s career path if they’ve overcome a problem.

Are there any barriers that you might want to keep?

Admiral CLARK. There may be, and if I were responsible for the policy review I would then look at all of the potential courses of action and make that kind of determination. But let me give you an example of the manner in which I might decide to handle the case you just suggested, because, as you correctly pointed out, by regulation there is some documentation that is not allowed to proceed from command to command.

We could figure out how to compartmentalize information. We do it in the intelligence world all the time. The briefer comes into the room with the material that’s in the pouch, that only certain people get to see that information. It would be very possible to have information that might be vital to connecting the dots that is currently not passed, passed in a way that’s compartmented so that a select group of people had access to the information.

I believe that that’s inherent in achieving the correct balance, Secretary West and I would not want anything that was said here to imply in any way that the balance between these issues isn’t—it’s very, very important. You have addressed it correctly. This is a challenge.

One of the hallmarks of the U.S. military is we grow and develop people. I’ve had dozens of these interviews with people: Okay, you’re getting a new job, this is turning over a new leaf, this is the time to go get it. We’ve seen people turn their lives around. This is one of the great things about our institution.

So clearly these are issues that the policymakers have to come to grips with. Our task was put the spotlight on policies, weaknesses, gaps, and that's what we have tried to do. I do believe that there may be places where barriers should be retained in some way.

Chairman LEVIN. Maybe for some purpose.

Admiral CLARK. For some purpose.

Chairman LEVIN. Maybe in a promotion.

Admiral CLARK. Exactly.

Chairman LEVIN. It's different from whether it's a strategic issue.

Admiral CLARK. Exactly. But what I'm suggesting is that people who are responsible for these policy decisions know what the vital dots look like, know where they come from. As the report says and I said in my earlier testimony, the time is passed for us to be having these turf wars on who owns the information.

Chairman LEVIN. I think we couldn't agree with you more, and this is a major challenge for all of us in the Senate and the House and our committees and, even more importantly probably, for the executive branch.

Senator Lieberman, do you want to add anything?

Senator LIEBERMAN. No, thanks.

Chairman LEVIN. We thank you for all the work you're doing, not just here but on the Homeland Security and Governmental Affairs Committee. That committee is doing critically important work.

We're now going to move to a closed session of the committee. We'll meet in room 222 in Russell, our committee room. In accordance with restrictions placed on access to the restricted annex, attendance will be limited to Senators and committee professional staff.

We again thank our witnesses, not just for their work in this regard, but for their lifelong work on behalf of our Nation.

The committee will stand adjourned.

[Questions for the record with answers supplied follow:]

#### QUESTIONS SUBMITTED BY SENATOR DANIEL K. AKAKA

##### INDICATORS FOR VIOLENCE

1. Senator AKAKA. Mr. West, research into the various predictors and causes of violence span many disciplines and offer varying perspectives regarding why some people resort to violence. These range from biological, to religious, social, and political factors. The four recommendations contained in 2.1 "Protecting the Force: Lessons from Fort Hood, Report of the Department of Defense (DOD) Independent Review, January 2010" (Independent Review) coalesce around the identification of contributing factors of violent actions and the reporting of behavioral indicators of violent actors. How must the DOD adequately update and strengthen programs, policies, processes, and procedures that address the identification of indicators for violence without violating the civil liberties that are enjoyed by the military members of the Armed Forces as well as DOD civilians?

Mr. WEST. The Department should thoughtfully consider a wide range of options and exercise due caution to avoid infringing on civil liberties. There are risk-assessment tools available for the Department's consideration that would enhance DOD's ability to deal with potential internal threats without compromising fundamental civil liberties. In particular, DOD should draw on the expertise of the law enforcement community, including the Federal Bureau of Investigation (FBI), which has developed methodologies to help understand the motivations and behaviors of violent offenders. My understanding is that the FBI has already been assisting DOD in understanding these issues.

We recommend that DOD continue to coordinate with the FBI Behavioral Science Unit, under their comprehensive analysis of military offenders project to identify behavioral indicators that are specific to DOD personnel that would be used to help protect against internal threats.

We also recommend that the Department develop tools and programs that would educate DOD personnel about indicators of possible violent behavior and help them determine the risk that such behavior might occur.

#### RELIGIOUS ACCOMMODATIONS

2. Senator AKAKA. Mr. West, recommendation 2.7 of the Independent Review states that the DOD should promptly establish standards and reporting procedures that clarify guidelines for religious accommodations. How must the DOD adequately clarify policy regarding religious accommodations to help commanders distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization while balancing the civil liberties that are enjoyed by the military members of the Armed Forces as well as DOD civilians?

Mr. WEST. The Department should issue clear guidance to provide a common source for commanders, supervisors, and chaplains to distinguish appropriate religious practices. The Department should exercise due caution to avoid infringing on civil liberties. Clear standards would ensure consistent mechanisms across the military departments, assisting commanders and supervisors in assessing behavior and initiating action, if appropriate.

#### HEALTH CARE PROVIDERS

3. Senator AKAKA. Admiral Clark, healthcare providers experience traumatic stress and provider burnout and are stigmatized when seeking treatment for stress and burnout. Other career fields, such as the Chaplaincy and their support personnel, have programs that assess stress and burnout. Recommendation 5.3 of the Independent Review states that the DOD should review its requirement to de-stigmatize healthcare providers who seek treatment. What steps should the DOD undertake to ensure the resiliency and recovery of healthcare providers so that they can continue to provide members of the Armed Forces and their families with the best healthcare?

Admiral CLARK. In order to ensure that healthcare providers can continue to provide outstanding care for warriors and their families as well as receive outstanding care themselves, DOD can take several steps to make certain that a good balance is being struck between health care for the warrior and health care for the provider. DOD's current deployment model, for example, should be reviewed to assess whether it provides sufficient continuity of care for redeploying servicemembers while not delaying recovery for health care providers who have been assigned to deploying combat units. DOD has a number of policies in place designed to guarantee that U.S. military forces receive top quality care and we are looking for further ways to integrate these policies and properly resource them to positively affect the Department's ability to continue delivering the best care available to all military members and their families.

#### OFFICERSHIP

4. Senator AKAKA. Admiral Clark, the joint opening statement refers to the fact that several individuals failed to apply professional standards of officership regarding the alleged perpetrator and that you recommended the Secretary of Defense forward these issues of accountability to the Secretary of the Army. How should the DOD address what the Independent Review characterizes as the failure to apply professional standards of officership and to make the reflection of an individual's total performance an accepted and standard practice throughout the Services?

Admiral CLARK. The conduct of Major Hasan's colleagues and former supervisors remains under review, and it would be inappropriate to comment at this time. Consistent with the recommendations of the Independent Review Panel, the Secretary of Defense referred issues of individual accountability to the Secretary of the Army for review and action as appropriate. Secretary McHugh assigned senior military leaders to investigate further, to assess accountability, and, as appropriate, to take final action. This process remains ongoing.

## QUESTIONS SUBMITTED BY SENATOR KAY R. HAGAN

## ACTIONS NOT TAKEN BY ARMY OFFICERS

5. Senator HAGAN. Mr. West and Admiral Clark, several officers failed to comply with existing Army policies when taking actions regarding the perpetrator, Major Hassan. There were also significant discrepancies between Major Hassan's performance in official records and his actual performance during training, residency, and fellowship. It seems that medical officers failed to include his overall performance as an officer, and instead, focused on his academic performance.

We have to ensure that performance appraisals accurately provide a holistic overview of professional, ethical, and personal career development of all personnel. Incomplete performance appraisals prevent us from recognizing vital warning signs in dealing with internal threats. They also prevent leaders from being alert to psychological and emotional risk factors of servicemembers and civilians. How should Secretary of Defense Gates and Secretary of the Army McHugh ensure accountability for those failures by some medical officers that did not apply appropriate judgment?

Mr. WEST and Admiral CLARK. Consistent with the recommendations of the Independent Review Panel, the Secretary of Defense referred issues of individual accountability to the Secretary of the Army for review and action as appropriate. Secretary McHugh assigned senior military leaders to investigate further, to assess accountability, and, as appropriate, to take final action. This process remains ongoing.

6. Senator HAGAN. Mr. West and Admiral Clark, why did Major Hassan's colleagues and former supervisors wait until after the Fort Hood incident to speak about the content of his extremist religious views?

Mr. WEST and Admiral CLARK. The conduct of Major Hasan's colleagues and former supervisors remains under review, and it would be inappropriate to comment at this time. Consistent with the recommendations of the Independent Review Panel, the Secretary of Defense referred issues of individual accountability to the Secretary of the Army for review and action as appropriate. Secretary McHugh assigned senior military leaders to investigate further, to assess accountability, and, as appropriate, to take final action. This process remains ongoing.

7. Senator HAGAN. Mr. West and Admiral Clark, what did the Army's higher authorities do when complaints were sent up the chain?

Mr. WEST and Admiral CLARK. The conduct of Major Hasan's colleagues and former supervisors remains under review, and it would be inappropriate to comment at this time. Consistent with the recommendations of the Independent Review Panel, the Secretary of Defense referred issues of individual accountability to the Secretary of the Army for review and action as appropriate. Secretary McHugh assigned senior military leaders to investigate further, to assess accountability, and, as appropriate, to take final action. This process remains ongoing.

## INTERAGENCY INFORMATION SHARING

8. Senator HAGAN. Mr. West and Admiral Clark, I agree that in order to protect the force, our civilian leaders and commanders in the field need immediate access to sensitive information regarding servicemembers' personal contacts, connections, or relationships with organizations promoting radicalization and violence. I encourage the Army and the DOD at-large to adopt the recommendation of the Independent Review to increase service representation on Joint Terrorism Task Forces and coordination with the FBI. What suggestions and recommendations can you offer to facilitate enhanced cooperation and information sharing between executive department agencies like the FBI, National Counterterrorism Center, Office of the Secretary of Defense, and the Army Secretariat?

Mr. WEST and Admiral CLARK. Liaison and information sharing agreements already exist among the executive department agencies you mention, but they can be strengthened. Many of these liaison and information sharing agreements currently focus on antiterrorism cooperation, potentially precluding the agencies from sharing sensitive information pertaining to a servicemember's propensity to commit violent acts. DOD should review the scope of these agreements to determine where they can appropriately be expanded and strengthened to enhance a commander's ability to assess his or her personnel.

We were pleased to learn that Secretary Gates approved our recommendation to establish a single organization within DOD to manage its participation in the Joint Terrorism Task Forces. We also are pleased the Secretary approved our rec-

ommendation to revise significantly DOD's Memorandum of Understanding with the FBI.

9. Senator HAGAN. Mr. West and Admiral Clark, what challenges do you foresee?

Mr. WEST and Admiral CLARK. First, revising interagency agreements is often a time-consuming process, particularly in the case of agreements that involve multiple interagency partners. Second, comprehensively accounting for all existing agreements will likely also be a time-consuming process. For example, in some cases, each Service has a separate agreement with a particular Federal agency on information sharing. Determining where these agreements differ, what the gaps are between them, and whether it is necessary or desirable to bring them under a single umbrella will be time consuming.

#### ENSURING THAT FORCE PROTECTION POLICIES COUNTER INTERNAL THREATS

10. Senator HAGAN. Mr. West and Admiral Clark, one of the most significant takeaways I got out of the Independent Review was that DOD force protection policies are not optimized for countering internal threats, and reflect a lack of awareness of the factors and indicators we have to be focused on in addressing internal threats.

I agree that we need to provide commanders with comprehensive guidance and a full range of indicators designed to effectively identify and address internal threats within the U.S. military establishment. Do you anticipate challenges in the military departments developing such guidance and indicators?

Mr. WEST and Admiral CLARK. We do not doubt that the military departments are committed to working to develop such guidance and indicators. That said, this is a complex undertaking, and we anticipate that it will be difficult to develop comprehensive guidance and a full range of indicators to address internal threats. The Department should thoughtfully consider a wide range of options and exercise due caution to avoid infringing on civil liberties. There are a number of recommendations that specifically address internal threats, including 2.1 (developing 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), 2.15 (review prohibited activities and recommend necessary policy changes), and 3.2 (commission a multidisciplinary group to examine and evaluate predictive indicators relating to pending violence and provide commanders with a multidisciplinary capability). It is our understanding that the Fort Hood Follow-On Review is addressing these recommendations to improve the Department's capacity to protect against internal threats.

11. Senator HAGAN. Mr. West and Admiral Clark, how will those indicators be coordinated with combatant commanders?

Mr. WEST and Admiral CLARK. Our understanding is that the Follow-On Review program includes representatives from all the military departments and the Joint Staff, which coordinates input from the combatant commands. As such, the combatant commands have a voice in determining how potential indicators will be coordinated with them. One of our recommendations was that the Department needs to develop standardized guidance regarding how military criminal investigative organizations and counter-intelligence organizations will inform the operational chain of command, e.g. the combatant commander. We understand the final report for the Follow-On Review will address this specific issue.

---

#### QUESTIONS SUBMITTED BY SENATOR ROLAND W. BURRIS

##### POTENTIAL THREATS

12. Senator BURRIS. Mr. West and Admiral Clark, are there other potential internal threats that our current system has failed to identify?

Mr. WEST and Admiral CLARK. We are not aware of other potential internal threats that the current system has failed to identify. However, our findings clearly show that DOD and Service programs that provide guidance concerning observation of personal behavior do not focus on internal threats. As such, one of our recommendations is to develop a list of behaviors that may be indicative of an insider threat and to integrate the disparate programs designed to defend against these threats.

13. Senator BURRIS. Mr. West and Admiral Clark, how can we identify potential sympathies which are counter to our national interests?

Mr. WEST and Admiral CLARK. In the Independent Review report, we recommended DOD promptly establish standards and reporting procedures that clarify guidelines for religious accommodation. 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 DOD.

#### FAILURES TO ACT

14. Senator BURRIS. Mr. West and Admiral Clark, in your investigation, were there other examples of a failure to act on performance reports and passing on the problem?

Mr. WEST and Admiral CLARK. The conduct of Major Hasan's colleagues and former supervisors remains under review, and it would be inappropriate to comment at this time. Consistent with the recommendations of the Independent Review Panel, the Secretary of Defense referred issues of individual accountability to the Secretary of the Army for review and action as appropriate. Secretary McHugh assigned senior military leaders to investigate further, to assess accountability, and, as appropriate, to take final action. This process remains ongoing.

---

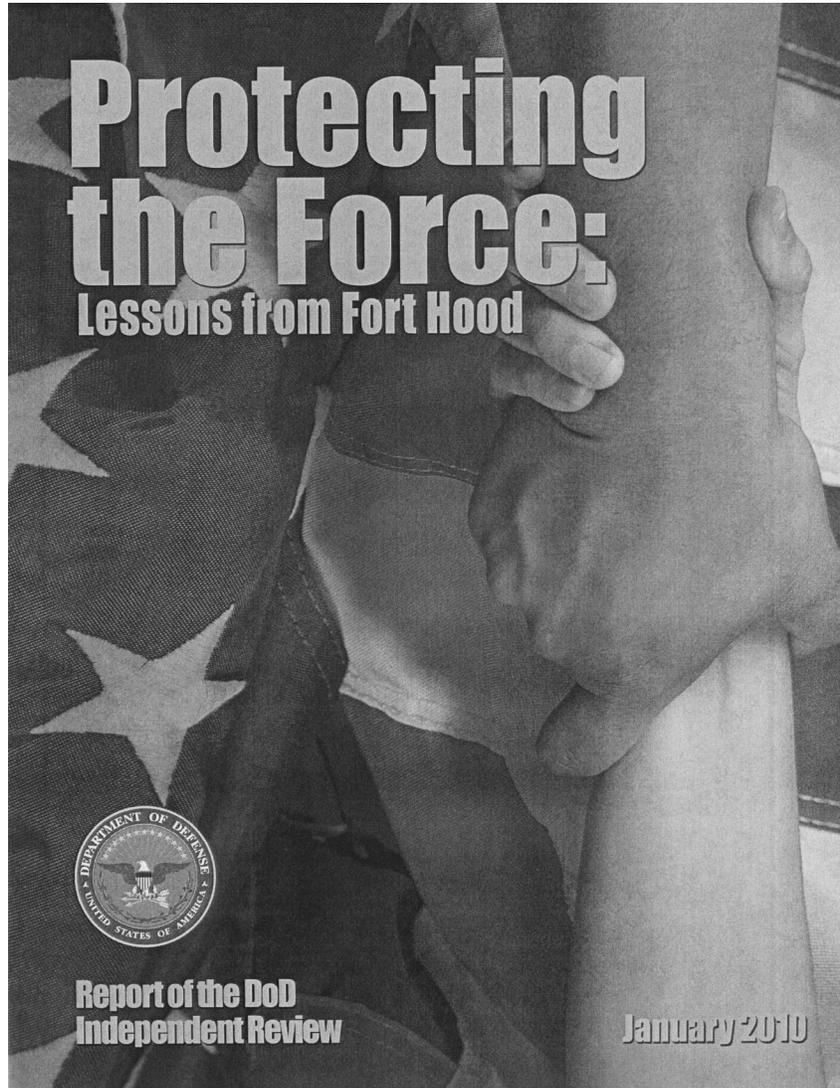
#### QUESTION SUBMITTED BY SENATOR DAVID VITTER

#### RECOMMENDATIONS

15. Senator VITTER. Mr. West and Admiral Clark, in Chapter 2 of the Independent Review, when reviewing barriers and constraints on taking action, you state that the existing authority to address potentially violent behaviors "is likely insufficient if an employee represents an imminent threat." However, your recommendations do not state specific changes to regulations that would enable the DOD and the Services to quickly adapt and address potential threats. Certainly identifying threats is important and critical to saving lives and preventing terrorist acts, but we must also prevent those threats after identifying them and cannot let bureaucratic polices stop us from averting terrorism. What specific policy changes at the company and battalion command level would you recommend to shorten commanders' response time in dealing with an immediate threat?

Mr. WEST and Admiral CLARK. In Chapter 4 of the Independent Review report, we identified several ways that the Department can better prepare its military communities to respond to emergencies, including developing a case study based on the Fort Hood incident to be used in installation commander development and on-scene commander response programs. But we also cannot discount the importance of responding to a potential threat immediately, before it becomes a violent action. Recommendation 2.1 specifically addresses updating policies and programs that would enable the DOD and Services to assess potentially violent behaviors. This includes developing 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. Recommendation 2.15 deals with reviewing prohibited activities and recommending necessary policy changes. For example, DOD can update DOD Instruction 1325.06, Handling Dissident and Protest Activities Among Members of the Armed Forces, by providing commanders and supervisors the guidance and authority to act on potential threats to good order and discipline. We defer to the Department on other policy changes it might identify and implement to improve commanders' response times in dealing with an immediate threat.

[Annex: The Report of the DOD Independent Review "Protecting the Force: Lessons from Fort Hood" follows:]



# 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

<b>Executive Summary</b> .....	1
Overview .....	1
Protecting the Force: Lessons from Fort Hood .....	2
Identifying Threats .....	3
Sharing Information .....	3
Force Security .....	4
Who is in Charge? .....	4
Reacting to the Event .....	4
The Alleged Perpetrator .....	6
Going Forward .....	7
<b>Chapter 1 Oversight of the Alleged Perpetrator</b> .....	9
<b>Chapter 2 Personnel Policies</b> .....	11
Indicators that DoD Personnel May Become a Danger to Themselves or Others .....	11
Reporting and Sharing Information About the Indicators .....	18
Barriers or Constraints on Taking Action .....	22
<b>Chapter 3 Force Protection</b> .....	25
Authorities/Command and Control .....	25
Indications and Warning .....	26
Information Sharing .....	28
Access Control .....	31
<b>Chapter 4 Emergency Response and Mass Casualty</b> .....	35
Emergency Response .....	35
Implementation of Enhanced 911 .....	36
Law Enforcement Practices—Active Shooter Threat .....	37
Mass Warning and Notification .....	39
Common Operational Picture .....	39
Synchronization of Emergency Management Policies and Programs .....	40
Mutual Aid Agreement .....	41
Emergency Family Assistance .....	43
Religious Support Integration .....	44
Memorial Service Support .....	46
Private Citizens with No DoD Affiliation .....	47
<b>Chapter 5 Support to DoD Healthcare Providers</b> .....	49
Mental Health Care Support .....	49

**Appendix A Memorandum and Terms of Reference** ..... A-1

**Appendix B Panel Roster** ..... B-1

**Appendix C Summary of Findings and Recommendations** ..... C-1

**Appendix D Literature Review of Risk Factors for Violence** ..... D-1

    Predicting Violent Behavior is a Long-Term Multi-Disciplinary Quest ..... D-1

    Risk Factors Vary Across Types of Violence ..... D-1

    Application for the Department of Defense ..... D-4

## 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.

## Executive Summary

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. 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.

**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.**

### 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

## Executive Summary

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.

## Executive Summary

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.

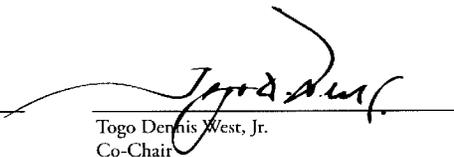
- Communicate immediately to the force, by direct message from the Secretary, the overriding requirement for commanders, supervisors, non-commissioned leaders, and fellow members of the force to reinforce the fabric of trust with one another by engaging, supervising, mentoring, counseling, and simple 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.

## 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.<sup>1</sup> Some populations (medical, legal, and chaplain officers who receive Direct Commissions into the Reserves<sup>2</sup> and some civilian employees<sup>3</sup>) 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.<sup>4</sup>

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

<sup>1</sup> 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.

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

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

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

## Chapter 2 Personnel Policies

character references.<sup>5</sup> 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.<sup>6</sup>

**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.<sup>7</sup> 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.<sup>8</sup> 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.

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

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

<sup>7</sup> “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, SECNAV 1 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.

<sup>8</sup> 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,<sup>9</sup> and

<sup>9</sup> 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.

## Chapter 2 Personnel Policies

specific guidance on a variety of high-risk health conditions.<sup>10</sup> Guidance on high-risk health conditions is 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<sup>11</sup> 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,<sup>12</sup> Sexual Assault Prevention & Response,<sup>13</sup> and Family Advocacy<sup>14</sup> programs address numerous facets of violence. Family Advocacy and Sexual Assault Prevention & Response programs

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

<sup>11</sup> 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.

<sup>12</sup> 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.

<sup>13</sup> 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.

<sup>14</sup> 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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup>

#### **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.<sup>18</sup> 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<sup>19</sup> applies to the military. Therefore, commanders, supervisors, and chaplains lack a common source to distinguish mainstream religious

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

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

<sup>17</sup> 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.

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

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

## Chapter 2 Personnel Policies

practices from extreme practices for faith groups. Service policies and procedures, therefore, vary in stating and reporting standards of religious accommodation.<sup>20</sup>

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.<sup>21</sup>

### 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

<sup>20</sup> 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, AFPPD 52-1, *Chaplain Service*, Washington, D.C., Oct. 2, 2006, 2.

<sup>21</sup> 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.<sup>22</sup> 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.<sup>23</sup> Some information included in these files is temporary, however, and is barred from becoming part of permanent records.<sup>24</sup> For example, Service policies place strong emphasis on commander discretion to record and/or forward information about minor law enforcement or disciplinary infractions.<sup>25</sup> 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.<sup>26</sup>

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<sup>27</sup>). 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.

## Chapter 2 Personnel Policies

must and/or cannot be maintained.<sup>28</sup> 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.

<sup>28</sup> 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.<sup>29</sup> 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.<sup>30</sup> 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.<sup>31</sup> Unique guidance on release of medical information has been established for Restricted Reporting in cases of sexual assault.<sup>32</sup>

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

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

<sup>31</sup> 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.A, *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.

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

## Chapter 2 Personnel Policies

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.<sup>33</sup> 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

<sup>33</sup> Department of Defense, D1M 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.<sup>34</sup> 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.<sup>35</sup> 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

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

<sup>35</sup> 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).

## Chapter 2 Personnel Policies

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.<sup>36</sup> 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.

<sup>36</sup> Department of Defense, DTM 09-006, *Revising Command Notification Requirements to Dipef Signos in Providing Mental Health Care to Military Personnel*, Washington, D.C., July 2, 2009, 1-6; Department of Air Force, AF1 36-704, *Discipline and Adverse Actions*, Washington, D.C., July 22, 1994, 13.

## 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.<sup>37</sup>

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.**

<sup>37</sup> 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.<sup>38</sup> 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.<sup>39</sup> 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

<sup>38</sup> 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.

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

## Chapter 3 Force Protection

**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.<sup>40</sup> 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.<sup>41</sup> 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.<sup>42</sup> The Association of Threat Assessment Professionals provides additional resources integrating academic, private, and public studies and programs for countering an insider threat.<sup>43</sup>

<sup>40</sup> 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 AALARACT 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.

<sup>41</sup> 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.

<sup>42</sup> United States Postal Service, Washington, D.C., May 1997.

<sup>43</sup> The Association of Threat Assessment Professionals, *The Association of Threat Assessment Professionals (ATAAP)*, <http://www.arapworldwide.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.<sup>44</sup> 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.<sup>45</sup>

**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.

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

<sup>45</sup> Department of Defense, DoDD 5106 01, *Inspector General of the Department of Defense*, Washington, D.C., Apr. 13, 2006.

## Chapter 3 Force Protection

### Discussion

*This relates to finding, discussion, and recommendation 2.10.*

Policy exists stating the requirement to share threat information with the Combatant Commands.<sup>46</sup> 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.<sup>47</sup>

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.<sup>48</sup> 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.

<sup>46</sup> 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.

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

<sup>48</sup> 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 JTF 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.

## Chapter 3 Force Protection

### 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.<sup>49</sup> 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.”<sup>50</sup> 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.

<sup>49</sup> 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.

<sup>50</sup> Department of Defense. DoD 5200.08-R. *Physical Security Programs: 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.<sup>51</sup>

**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

<sup>51</sup> 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, AF131-101 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.

## Chapter 3 Force Protection

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.

## 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.<sup>52</sup> 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.<sup>53</sup> 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.<sup>54</sup> 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.

<sup>52</sup> 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.

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

<sup>54</sup> *Ibid.*

Current Air Force guidance<sup>55</sup> 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.<sup>56</sup> 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.<sup>57</sup>

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),<sup>58</sup> 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<sup>59</sup> 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.

<sup>55</sup> 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.

<sup>56</sup> 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.

<sup>57</sup> 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.

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

<sup>59</sup> 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.

## Emergency Response and Mass Casualty

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.<sup>60</sup>

## 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.<sup>61</sup> 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.

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.<sup>62</sup> After Columbine, police departments collectively developed new active shooter response protocols with the goal being to neutralize the threat immediately. The Fort Hood AAR<sup>63</sup> 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.<sup>64</sup>

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

<sup>60</sup> 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.

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

<sup>62</sup> 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.

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

<sup>64</sup> 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.lastate.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.<sup>65</sup> 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.<sup>66</sup> 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*.<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup>

#### **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.<sup>70</sup>
- Develop a case study based on the Fort Hood incident to be used in installation commander development and on-scene commander response programs.

<sup>65</sup> Department of Defense. DoDI 5210.90, *Mutualism Training, Certifications, 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.

<sup>66</sup> 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.

<sup>67</sup> 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."

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

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

<sup>70</sup> *Ibid.*

## Emergency Response and Mass Casualty

### 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.”<sup>71</sup> *DoD Antiterrorism Standards* also require that mass notification systems be incorporated into emergency response planning.<sup>72</sup> The specific standards, requirements, and applications for all mass notification systems are contained in the Unified Facilities Criteria.<sup>73</sup>

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.*<sup>74</sup>

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.<sup>75</sup> 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.<sup>76</sup>

#### 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.<sup>77</sup>

<sup>71</sup> Department of Defense. DoDI 6055.17, *DoD Installation Emergency Management Program*. Washington, D.C., Jan. 13, 2009, 32.

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

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

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

<sup>75</sup> Department of the Navy. Draft CNIC Instruction 2000.XX, *CNIC Wide Area Alert Network*. Unpublished, Paragraph 5.0, System Operational Requirements.

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

<sup>77</sup> 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."<sup>78</sup> 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,"<sup>79</sup> 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.<sup>80</sup>

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.

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

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

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

## Emergency Response and Mass Casualty

- 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.<sup>81</sup> 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<sup>82</sup> 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.

<sup>81</sup> 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.

<sup>82</sup> 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<sup>83</sup> requires military treatment facilities to meet or exceed the accreditation standards of The Joint Commission (TJC)<sup>84</sup> 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.<sup>85</sup> 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.<sup>86</sup>

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<sup>87</sup> and to be signed by a responsible official.<sup>88</sup>

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.<sup>89</sup> 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

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

<sup>84</sup> 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](http://www.jointcommission.org/aboutus/joint_commission_history.htm), (accessed Dec. 9, 2009).

<sup>85</sup> 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,

<sup>86</sup> Department of Defense. DoDI 6055.17, *Installation Emergency Management Program*, Washington, D.C., Jan. 13, 2009.

<sup>87</sup> 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.

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

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

## Emergency Response and Mass Casualty

**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.<sup>90</sup> 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.<sup>91</sup>

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.<sup>92</sup>

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

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

<sup>91</sup> Ibid.

<sup>92</sup> 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.

<sup>93</sup> 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.<sup>94</sup>

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.<sup>95</sup> 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.<sup>96</sup> 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.<sup>97</sup> 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.<sup>98</sup> Other than the Army Medical

<sup>94</sup> Airman and Family Readiness Center. *Emergency Family Assistance Control Center Tool Kit*. May 2007.

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

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

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

<sup>98</sup> U.S. Marine Corps. MCRP 6-12A, *Religious Ministry Team Handbook*. Quantico, VA, May 16, 2003, 5-1, 3-9.

## Chapter 4

**Emergency Response and Mass Casualty**

Command's regional Special Medical Augmentation Response Teams,<sup>99</sup> 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<sup>100</sup> designate the chaplain as a formal member of the installation emergency management planning team, the Critical Incident Stress Management Team, the Disaster Response Force,<sup>101</sup> and the Disaster Response Team.<sup>102</sup> 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.<sup>103</sup> 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.

<sup>99</sup> 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.

<sup>100</sup> 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.

<sup>101</sup> 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.

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

<sup>103</sup> 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.<sup>104</sup>

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.<sup>105</sup>

**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.<sup>106</sup> 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.

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

<sup>105</sup> Presentation at Fort Hood, TX, Dec. 8, 2009.

<sup>106</sup> 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.

## Emergency Response and Mass Casualty

### Private Citizens with No DoD Affiliation

#### Finding 4.12

- DoD casualty affairs policy,<sup>107</sup> Federal law,<sup>108</sup> and DoD mortuary affairs guidance<sup>109</sup> 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.<sup>110</sup> In the area of DoD and Service mortuary affairs policies, this review revealed a similar absence of guidance regarding mortuary entitlements and services.<sup>111</sup>

#### 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.

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

<sup>108</sup> Federal Law, Title 5, United States Code, Section 5742, *Transportation of Remains, Dependents and Effects: Death Accruing Away From Installation or Abroad*. Washington, D.C.: Jan. 5, 2009.

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

<sup>110</sup> 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 Procedures 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.

<sup>111</sup> 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.

## 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.<sup>112</sup> 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<sup>113</sup> that incorporated current practices including a “whole of community” approach, and a strategy for long-term behavioral healthcare not reflected in any DoD policy.

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

<sup>113</sup> 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.<sup>114</sup> 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,<sup>115</sup> the Department of Defense Task Force on Mental Health, and the Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury.<sup>116</sup>

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.<sup>117</sup>
- A standardized provider training curriculum for treating post traumatic stress disorder.<sup>118</sup>
- 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.<sup>119</sup>
- 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.<sup>120</sup>

## 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.<sup>121</sup>

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

<sup>115</sup> Uniformed Services University of the Health Sciences, *Department of Psychiatry*. <http://www.usuhs.mil/psych/fellowships.html>. (accessed Dec 10, 2009).

<sup>116</sup> 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).

<sup>117</sup> 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.

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

<sup>119</sup> 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).

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

<sup>121</sup> 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.

## Support to DoD Healthcare Providers

### 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.<sup>122</sup> 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.<sup>123</sup>

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

<sup>123</sup> 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.<sup>124</sup> 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.<sup>125</sup> It is equally important to enhance the resiliency and recovery of care providers.<sup>126</sup> 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.<sup>127</sup>

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

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

<sup>126</sup> *Ibid.*

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

## 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.<sup>128</sup>

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.<sup>129</sup> 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.

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

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

## 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 perpetrator.

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

## Memorandum and Terms of Reference

### **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 perpetrator.

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 perpetrator.
  - 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.

**Appendix A****Memorandum and Terms Of Reference**

- 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.

## 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 Clemons, 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

LCDR James Cannon, PhD, PA, USCG  
 SGM Devon Matthew, USA  
 SMSgt Glynda Lilly, USAF  
 Mr. Dale Hamby  
 Ms. Mary Woodward

**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

## **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.

## Appendix C

**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.

## Summary of Findings and Recommendations

**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

## Appendix C

**Summary of Findings and Recommendations**

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.<sup>1</sup> 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.<sup>2</sup>

Most research to date has been conducted on physical violence perpetrated by individuals.<sup>3</sup> 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. Lucigio, “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.<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup>

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

Recent research has focused on why individuals become terrorists.<sup>10</sup> Although some people self-radicalize as individuals, more commonly small groups of people self-radicalize together.<sup>11</sup> Group dynamics can foster the dehumanization of targets and the drive to commit violence.<sup>12</sup> 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.<sup>13</sup>

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

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, Kathryn 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-Cuena 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-Cuena 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,” *NJI 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.

## Appendix D

**Literature Review of Risk Factors for Violence**

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.<sup>16</sup>

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.<sup>17</sup> The risk for intimate partner homicides is higher in homes with domestic violence, firearms, and illicit drug use.<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup>

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.<sup>21</sup> 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.<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup>

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](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 Roberttello 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.<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup> Research on homicide is better developed than research on multiple homicides, such as serial killing, spree killing, and mass murder.<sup>28</sup>

## 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 report. 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.<sup>29</sup> 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

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

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

<sup>27</sup> *Ibid.*

<sup>28</sup> An Crabbé, Stef Devoene, 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 Puthmann, and Mark T. Berg, "The Storkweather 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.

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

## Appendix D

**Literature Review of Risk Factors for Violence**

incorporating this model was quite accurate in its assessment of whether patients fell into a low- or high-risk group for violence.<sup>30</sup> This software, called Classification of Violence Risk, is available for use with acutely hospitalized civil patients,<sup>31</sup> 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.<sup>32</sup> 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 Koziel-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* 25:0 (2003): 14-19.

**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 Clemons, 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



[Whereupon, at 12:00 p.m., the committee adjourned.]

○