LESSONS FROM FORT HOOD: IMPROVING OUR ABILITY TO CONNECT THE DOTS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 14, 2012

Serial No. 112–118

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

81–127 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT

MICHAEL T. MCCAUL, Texas, *Chairman*

GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

WILLIAM R. KEATING, Massachusetts
YVETTE D. CLARKE, New York
DANNY K. DAVIS, Illinois
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DR. R. NICK PALARINO, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Director*

CONTENTS

LESSONS FROM FORT HOOD: IMPROVING OUR ABILITY TO CONNECT THE DOTS

Friday, September 14, 2012

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND MANAGEMENT,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 9:12 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the subcommittee] presiding.

Present: Representatives McCaul, Duncan, Keating, and Davis.

Mr. MCCAUL. The committee will come to order.

The purpose of this hearing is to examine information sharing across relevant intelligence and law enforcement agencies, specifically as it pertains to the report issued by the Webster Commission, which focused on the Fort Hood attack. As I mentioned, Mr. Winter, let me applaud you for your great work, and Mr. Webster, on that report.

I now recognize myself for an opening statement.

Before we begin today's hearing, we should pay tribute to our brave diplomats who serve our Nation abroad. Unfortunately, one of our ambassadors, Chris Stevens, and three of his colleagues were killed on Tuesday, the 11th anniversary of the 9/11 attacks on the United States. These events and others should remind every American that we are a Nation under siege and must remain vigilant, doing all that we can to uncover and take action against terrorist plots, whether the danger confronts us here in the United States or abroad.

In June 2009, FBI Director Robert Mueller acknowledged the immense challenge facing the Bureau, stating, "It is not sufficient for us as an organization to respond to a terrorist attack after it has occurred. It is important for us as an organization to develop the intelligence to anticipate a terrorist attack, developing intelligence, developing facts. In the past, we looked at collecting facts for the courtroom. We now have to think of ourselves as gathering facts and painting a picture of a particular threat, understanding the risk and moving to reduce that risk." I couldn't agree more with the Director's statement.

Then on November 5, 2009, a gunman walked into the Soldier Readiness Center at Fort Hood, Texas, and shouted the classic jihadist term "Allahu Akbar" and opened fire on unarmed soldiers and civilians. He killed 13 and wounded 42 others. This was the most horrific terrorist attack on U.S. soil since 9/11.

Today, we will examine the facts of the Fort Hood case as we know them to better understand how these facts that seem so obviously alarming now were so missed by seasoned professionals and to understand how the FBI and intelligence community as a whole can benefit from the lessons learned from this tragedy at Fort Hood.

The suspect in the Fort Hood shooting is Major Nidal Hasan, a commissioned officer in the United States Army, who openly communicated with the Muslim cleric and No. 2 terrorist Anwar al-Awlaki. Hasan characterized himself as a soldier of Allah and who was assigned the task of counseling our soldiers coming home from the battlefield.

Let's step back in time and examine the facts.

On May 31, 2009, Hasan sent one of several emails to al-Awlaki, one of the ones that I found most disturbing. The email read in part, "I heard a speaker defending suicide bombings as permissible. He contends that suicide is permissible in certain cases. He defines suicide as one who purposely takes his own life but insists that the important issue is your intention. Then he compares this to a soldier who sneaks into an enemy camp during dinner and detonates his suicide vest to prevent an attack that is known to be planned the following day. The suicide bomber's intention is to kill numerous soldiers to prevent the attack to save his fellow people the following day. He is successful. His intention was to save his people, his fellow soldiers, and the strategy was to sacrifice his life. This logic seems to make sense to me," says Mr. Hasan.

This email telegraphs almost precisely what happened that fateful day. This email was in the hands of the FBI before the attack.

In another email to Anwar al-Awlaki, Hasan asked, "Please keep me in your Rolodex in case you find me useful, and please feel free to call me collect."

So in December, 2008, the FBI's San Diego field office intercepted two emails from Hasan and al-Awlaki and identified the email as a product of interest. Over the course of the next several months, the San Diego field office and the Washington field office would exchange emails about how aggressively to investigate the Hasan lead.

In June 2009, Washington sent the following email to San Diego: "Given the context of his military and medical research and the content of his, to date, unanswered email messages from al-Awlaki, WFO does not currently assess Hasan to be involved in terrorist activities."

The FBI agent in San Diego described Washington's inquiry into Major Hasan as "slim."

The case was dropped until November 5, when the media began circulating reports of the massacre. At that time, the San Diego agents knew exactly who the perpetrator was, saying, "You know who that is. That's our boy."

Years before the FBI knew of Nidal Hasan, the Army major was being noticed by his superiors and colleagues at Walter Reed Army Medical Center, where he was a resident in the psychiatric program being trained to care for soldiers coming home from war. Two fellow officers described Hasan as a, "ticking time bomb."

During his medical residency and post-residency fellowship, Hasan demonstrated evidence of violent extremism. On several occasions he presented sympathetic views towards a radical Islam view and wrote papers defending Osama bin Laden, actions that enraged his classmates and professors. Yet no action was taken. Instead, Major Hasan was rewarded for his work and promoted.

His officer evaluation reports state, "Among the better disaster and psychiatry fellows to have completed the master of public health at the Uniformed Services University. He has a keen interest in Islamic culture and faith and has shown capacity to contribute to our psychological understanding of Islamic nationalism and how it may relate to events of National security and Army interest in the Middle East and Asia."

These officer evaluation reports were inaccurate. These were all flags, none of which were acted upon. So many flags in this case. These reports did not present the facts about Hasan's character. In reality, Hasan was barely a competent psychiatrist, whose radical views alarmed his colleagues; and the irony to me is this is the very man who was to counsel our soldiers coming back from the field of battle.

In the Hasan case, both the FBI and DOD had important pieces to the puzzle that, if put together, maybe just could have possibly saved the lives of 12 soldiers and one civilian.

I want to personally express my sympathy to those impacted by the terrorist attack at Fort Hood. We should treat those who died and who were wounded as brave Americans and award each of them a Purple Heart medal.

When I spoke with the victims' families at the Fort Hood memorial service, I saw first-hand the outrage and loss they felt, and I wanted to help them find answers. But I want these answers to serve as a catalyst to effect change and improve our intelligence community as a whole so we can stop these attacks before they occur. We have had great successes. We do look forward to hearing from the witnesses' testimonies to understand what went wrong in this case and how we can prevent such a tragedy from occurring in the future.

With that, I now recognize the Ranking Member, the gentleman from Massachusetts, Mr. Keating.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

SEPTEMBER 14, 2012

Before we begin today's hearing we should pay tribute to our brave diplomats who serve our Nation abroad. Unfortunately one of Ambassadors, Christopher Stevens, and three of his colleagues were killed on Wednesday, the eleventh anniversary of the 9/11 attacks on the United States. These events, and others, should remind every American that we are a Nation under siege and must remain vigilant doing all we can to uncover and take action against terrorists, whether the danger confronts us here in the United States or abroad.

In June 2009, Federal Bureau of Investigation (FBI) Director Robert Mueller acknowledged the immense challenges facing the Bureau stating:

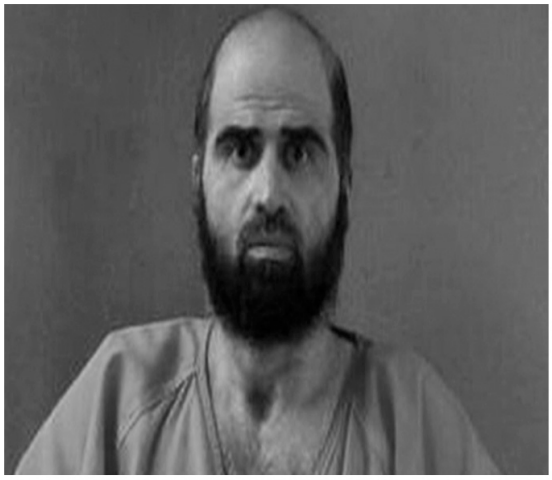
"The stages we are going through now I call mind-set changes. By mind-set I mean understanding that it is not sufficient for us as an organization to respond to a terrorist attack after it has occurred. It is important for us as an organization to develop the intelligence to anticipate a terrorist attack. Developing intelligence is developing facts. In the past we looked at collecting facts for the courtroom. We now

have to think of ourselves as gathering facts and painting a picture of a particular threat, understanding the risk and moving to reduce that risk."

On November 5, 2009, a gunman walked into the Soldier Readiness Center at Fort Hood, Texas, shouted "Allah Akbar," and opened fire on unarmed personnel. He killed 13 and wounded 42 others. This was the most horrific terrorist attack on U.S. soil since 9/11.

Today we will examine the facts of the Fort Hood case as we now know them—to better understand how these facts that seem so obviously alarming now were missed by seasoned professionals—and to understand how the FBI and intelligence community as a whole can benefit from the lessons learned from the tragedy at Fort Hood.

The suspect in the Fort Hood shootings is Major Nidal Malik Hasan, a commissioned officer in the United States Army, who openly communicated with the terrorist Anwar al-Awlaki, who characterized himself as a soldier of Allah, and who was assigned the task of counseling our soldiers coming home from the battlefield.



US Army Major Nidal Malik Hasan

Let's step back in time and examine the facts. On May 31, 2009, Hasan sent one of several emails to the radicalized Muslim cleric Anwar al-Alwaki. The email read:

"I heard a speaker defending suicide bombings as permissible . . . He contends that suicide is permissible in certain cases . . . He defines suicide as one who purposely takes his own life but insists that the important issue is your intention . . . Then he compares this to a soldier who sneaks into an enemy camp during dinner and detonates his suicide vest to prevent an attack that is known to be planned the following day. The suicide bomber's intention is to kill numerous soldiers to prevent the attack to save his fellow people the following day. He is successful. His intention was to save his people/fellow soldiers and the strategy was to sacrifice his life. The logic seems to make sense to me . . . "

"I heard a speaker defending suicide bombings as permissible …. He contends that suicide is permissible in certain cases. … He defines suicide as one who purposely takes his own life but insists that the important issue is your intention. … Then he compares this to a soldier who sneaks into an enemy camp during dinner and detonates his suicide vest to prevent an attack that is known to be planned the following day. The suicide bombers intention is to kill numerous soldiers to prevent the attack to save his fellow people the following day. He is successful. His intention was to save his people/fellow soldiers and the strategy was to sacrifice his life. The logic seems to make sense to me …"

In another email to al-Awlaki, Hasan asks to "Please keep me in your Rolodex in case you find me useful and feel free to call me collect."

In December 2008, the FBI San Diego Field Office intercepted two emails from Hasan to al-Awlaki and identified the email as "Product of Interest." The lead was sent to the Washington field office because Hasan resided in the area. Over the course of the next several months the San Diego field office and the Washington field office would exchange emails about how aggressively to investigate the Hasan lead. In June 2009, the Washington field office sent the following email to the San Diego field office:

"Due to [redacted] HASAN'S email contact with AULAQI, HASAN was not contacted, nor were his command officials. Given the context of his military/medical research and the content of his, to date unanswered [from AULAQI] email messages, WFO does not currently assess HASAN to be involved in terrorist activities."

"…given the context of his military/medical research and the content of his, to date unanswered [from AULAQI] email messages, WFO does not currently assess HASAN to be involved in terrorist activities."

The FBI agent in San Diego described Washington's inquiry into Hasan "slim". The case was dropped until on November 5 when the media began circulating reports of the massacre—the San Diego agents knew immediately saying, "you know who that is, that's our boy."

Years before the FBI knew of Nidal Hasan the Army Major was being noticed by his superiors and colleagues at Walter Reed Army Medical Center where he was a resident in the psychiatric program being trained to care for soldiers coming home from war. Two fellow officers described Hasan as a "ticking time bomb". During his medical residency and post-residency fellowship Hasan demonstrated evidence of violent extremism. On several occasions, he presented sympathetic views towards radical Islam and wrote papers defending Osama bin Laden—actions that enraged his classmates and professors. Yet no action was taken.

Instead, Major Hasan was rewarded for his work and promoted. His officer evaluation reports state:

" . . . among the better disaster and psychiatry fellows to have completed the Master of Public Health at the Uniformed Services University"

" . . . keen interest in Islamic culture and faith and has shown capacity to contribute to our psychological understanding of Islamic nationalism and how it may relate to event of National security and Army interest in the Middle East and Asia."

"… among the better disaster and psychiatry fellows to have completed the Master of Public Health at the Uniformed Services University.

… keen interest in Islamic culture and faith and has shown capacity to contribute to our psychological understanding of Islamic nationalism and how it may relate to event of national security and Army interest in the Middle East and Asia."

These officer evaluation reports were inaccurate. They did not present the facts about Hasan's character. In reality, Hasan was barely a competent psychiatrist whose radical views alarmed his colleagues.

In the Hasan case, both the FBI and DOD had important pieces to the puzzle that if put together could have developed the picture more accurately and in my opinion, would've prompted a more thorough inquiry. Of course, we don't know if that could've changed the events at Fort Hood but we should strive to improve, for the victims and their families.

I want to personally express my sympathy to those impacted by the terrorist attack at Fort Hood. We should treat those who died and were wounded as brave Americans and award each a Purple Heart Medal.

When I spoke with the victims' families at the Fort Hood Memorial service, I saw first-hand the outrage and loss they felt and I want to help them find answers. But I want the answers to serve as a catalyst to affect change and improve our intelligence community as a whole so we can stop these attacks before they occur.

We look forward to hearing the witness testimonies to better understand what went wrong and how we can prevent such tragedies in the future.

Mr. KEATING. Thank you, Mr. Chairman.

As we all pause to think of the families of the four Americans who were lost just this week in Libya and keep their families in our prayers and thoughts, it is significant that we come here today in dedication to find every piece of information we can find that will determine how better to keep the Americans that serve us so well safe as they try to keep us safe. So with that, Mr. Chairman, I thank you for holding today's hearing.

Three years ago, on November 5, 2009, the Nation was shocked by the mass shooting that occurred at the Army Deployment Center located at Fort Hood, Texas. During the shooting, 13 lives were lost, 43 individuals were wounded, and the lives of so many others were forever changed.

It later became evident that the warning signs existed well before the tragedy and should have, at a minimum, been further investigated. Both the FBI and the Department of Defense had

knowledge of Major Hasan's potential as a threat to homeland security.

The actions leading up to the massacre by Major Nidal Malik Hasan, the sole suspect in the murders, should have unequivocally sparked a greater concern on the part of officials. Yet dots were not connected, information was not shared, and the lack of formal policies and protocols led to a colossal breakdown in communication.

In December, 2009, at the direction of the FBI director, the Webster Commission was created to examine the events that occurred before and after the shootings. The Final Report of the William H. Webster Commission on the FBI, Counterterrorism Intelligence, and the Events at Fort Hood Texas, which represent the work of the Commission, was released in July 2012.

The crucial recommendation mirrored in both the Webster Commission's report and the 9/11 Commission's report focused on the importance of information sharing to our Nation's security and the need to do away with a culture of territorialism that existed between the various levels of Federal, State, and local authorities. As a former Massachusetts district attorney myself, I was once at the bottom rung of the information-sharing ladder and understand the consequences of inadequate lines of communication. For this reason, my first legislative measure signed into law was an amendment to the intelligence authorization that encouraged Federal authorities to utilize fusion centers and enlist all of the intelligence capabilities, including that of law enforcement, to secure our homeland.

Since then, I have been following the progress of the recommendations set forth in the 9/11 Commission, and now the Webster Commission, in regard to intelligence sharing and am pleased that the administration has indicated that effective information sharing and access throughout the Government is a top priority.

This all being said, I am interested in hearing from both our witness panels today on their thoughts and their own recommendations.

With that, I yield back the balance of my time.

[The statement of Ranking Member Keating follows:]

STATEMENT OF RANKING MEMBER WILLIAM KEATING

SEPTEMBER 14, 2012

Three years ago, on November 5, 2009, the Nation was shocked by the mass shooting that occurred at the Army deployment center located at Ft. Hood, Texas. During the shooting, 13 lives were lost, 43 individuals were wounded, and the lives of so many others were forever changed. It later became evident that warning signs existed well before this tragedy and should have, at a minimum, been further investigated.

Both the FBI and the DOD had knowledge of Major Hasan's potential as a threat to homeland security. The actions leading up to the massacre by Major Nidal Malik Hasan—the sole suspect in the murders—should have unequivocally sparked greater concern.

Yet, dots were not connected, information was not shared, and the lack of formal policies and protocols led to a colossal breakdown in communication.

In December 2009, at the direction of the FBI Director, the Webster Commission was created to examine the events occurring before and after the shootings.

The Final Report of the William H. Webster Commission on the FBI, Counterterrorism Intelligence, and the Events at Fort Hood, Texas which represents the work of the Commission was released in July 2012.

The crucial recommendation mirrored in both the Webster Commission's report and the 9/11 Commission's report focused on the importance of information-sharing to our Nation's security and need to do away with the culture of territorialism that existed between the various levels of Federal, State, and local authorities.

As a former Massachusetts District Attorney, I was once on the bottom rung of the information-sharing ladder and understand the consequences of inadequate lines of communication.

For this reason, my first legislative measure that was signed into law was an amendment to the Intelligence Authorization that encouraged Federal authorities to utilize fusion centers and enlist all of the intelligence capabilities—including that of law enforcement—to secure our homeland.

Since then I have been following the progress of the recommendations set forth by the 9/11 Commission, and now the Webster Commission, in regard to intelligence-sharing and am pleased that the administration has indicated that effective information sharing and access throughout the Government is a top priority. This all being said, I am interested to hear from both witness panels today on their thoughts and their own recommendations.

Mr. MCCAUL. I thank the Ranking Member. Members are reminded that additional statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 14, 2012

Three days ago, we marked the eleventh anniversary of the September 11, 2001 terrorist attacks.

That tragedy left us with a number of valuable lessons. As the 9/11 Commission found, Government agencies charged with collecting intelligence and law enforcement data did not "connect the dots" that could have revealed that attacks of the proportion launched on 9/11 were under way.

Since that time, the importance of horizontal information sharing among Federal agencies and vertical information sharing from Federal agencies to State, local, and Tribal entities has been weaved into our homeland security efforts.

However, on November 5, 2009, the tragic events that occurred at the Army base located in Fort Hood, Texas, once again revealed that the failure to connect the dots can lead to disastrous results.

On that day, 13 people lost their lives and 43 individuals were wounded at the hand of a single gunman who was on the separate radars of the FBI and the DOD. Unfortunately, that information was not coordinated.

In some of the reports and the rhetoric following the Ft. Hood shooting, there were claims that the failure to connect the dots was based on "political correctness."

I strongly disagree. The information-sharing challenges that we faced then and continue to face now are more grounded in protecting turf than being timid.

To conclude that the source of the missteps was based on the religion of the perpetrator takes us backwards and takes our eyes off the ball.

Instead, our focus should be on ensuring that communication systems, information technology, training, and protocols are improved Government-wide.

And most importantly, removing stovepipes.

The Fort Hood shooting occurred nearly 3 years ago. Fortunately, since that time, information sharing has improved and we have the death of Osama bin Laden, the conviction of the New York City subway bomber, and other success stories as proof of this joint effort.

Mr. MCCAUL. We are pleased to have a very distinguished panel of witnesses here today, and I would like to introduce them.

First, we have Mr. Douglas Winter. He is Deputy Chair and Editor-in-Chief of the William Webster Commission. He is a counsel and former partner in the law firm of Bryan Cave, where he is the head of the firm's electronic discovery unit. He served as law clerk to Judge William Webster on the U.S. Court of Appeals for the 8th Circuit. Also served as a captain in the U.S. Army and is a graduate of the U.S. Army Judge Advocate General school.

Second, we have Ms. Irshad Manji. She is the Director of Moral Courage Project at New York University's Wagner Research Center for Leadership in Action. As Director, she equips students to become global citizens by speaking truth to power in their communities. As a reformist Muslim, Ms. Manji has written multiple books on the trends that are changing the world of Islam.

It is so great to have you here today. Thank you for being here.

Finally, I would say my colleague and friend from Department of Justice, Mr. Leiter. Michael Leiter is the Senior Counsel to the Chief Executive Officer of Palantir Technologies and the former Director of the National Counterterrorism Center.

It is great to have you here today as well, Mr. Leiter.

The Chairman now recognizes Mr. Winter for his testimony.

STATEMENT OF DOUGLAS E. WINTER, DEPUTY CHAIR, THE WILLIAM H. WEBSTER COMMISSION

Mr. WINTER. Thank you.

Good morning, Chairman McCaul, Ranking Member Keating, and Members of the subcommittee. I am joined today by Adrian Steel, the commissioner who was responsible as governing authorities liaison with the Department of Justice and the FBI, and also staff member George Murphy.

It is impossible in the time allotted to describe the lengthy and detailed investigation that is set forth in the final report. Director Mueller's terms of reference were extraordinary in scope.

The factual background, as you know, is intricate and complex. There is no simple calculus of cause and effect here. The mistakes and shortcomings we identified were the products of cascading sets of circumstances that range from a lack of policy guidance, training, and adequate technology to a misleading set of Army personnel records and an error in interpreting an abbreviation.

My written statement sets forth an overview of our analysis and our findings. Today, I will devote a review of the recommendations to help underscore the lessons of Fort Hood.

The FBI has concurred in the principles underlying each of our 18 recommendations and in almost every instance has implemented or is implementing a responsive measure. We recommended that the FBI adopt seven policies to formalize FBI practices that were not followed in the Hasan matter or that would help assure information sharing in similar circumstances. The recommended policies concerned the counterterrorism command-and-control hierarchy at the FBI, restrictions on counterterrorism leads assigned to Joint Terrorism Task Force officers, and clearinghouse procedures for counterterrorism investigations and assessments of law enforcement personnel and other Government personnel.

When Judge Webster was sworn in as director of the FBI, there were three analysts at the FBI. Today, the FBI relies on a cadre of more than 3,000 intelligence analysts with established career paths. We applauded the FBI's success in embedding analysts, creating fusion cells, and other analysis-driven initiatives. We recommended further integration of analysts into FBI operational groups.

A crucial lesson of Fort Hood is the ever-changing diversity and complexity of communications technologies and the impact of the

ever-growing amount of electronic information on the FBI's ability to identify and combat terrorism. These change the ways in which the FBI will in the future need to acquire, store, review, manage, disseminate, and act on intelligence.

We recommended that the FBI expedite and seek expanded funding for enterprise data management programs, with an emphasis on aggregating its primary investigative databases, collecting and storing data as a separate service from applications, and developing shared storage solutions across the U.S. intelligence community.

We recommended that the FBI seek funding for acquisition of new hardware for its DWS–EDMS database system, which lacks the infrastructure to fulfill system demands and also lacks a live disaster recovery backup.

Only two people, an FBI agent and an analyst, were charged with reviewing information in the al-Awlaki investigation. The crushing volume of information they confronted, the limited technology, and other factors forced those two people to review the 18 Hasan-al-Awlaki communications in a day-to-day context with 20,000 other items of electronic information they reviewed.

We recommended that the FBI evaluate and acquire information technology that was automated and advanced that would assist personnel in reviewing and managing data.

We also recommended that the FBI implement managed information review protocols for these types of large data collections. That would allow for case-specific review of the type that occurred in the al-Awlaki investigation, as well as strategic review by different review teams.

An important reminder of Fort Hood is that Congress, the Justice Department, and the FBI must assure that the FBI's governing authorities strike an appropriate balance between protecting civil liberties and privacy interests and detecting and deterring threats like those posed by Major Hasan. We recommended, among other things, that the FBI should increase internal compliance reviews and audits and that its existing governing authorities should remain in effect.

Training, we learned, is crucial, particularly in the task force context, where you have a diverse number of Federal, State, local, and Tribal agencies. The DCIS agent who conducted the Hasan assessment in the Washington field office did not even know that the DWS–EDMS database existed, leading him, and in turn his FBI supervisor, to believe that there were only two communications between Hasan and al-Awlaki. We recommended that the FBI require task force officers to complete database and computer training before they join the Joint Terrorism Task Force.

In closing, I want to note that the final report focuses on what went wrong. But throughout our investigation we were witness to all that was right about the FBI. We saw patriotism, professionalism, dedication, and long hours of work in a context of constant threats and limited resources. Agents, analysts, and task force officers are confronted with decisions every day whose consequences may be life or death. These personnel need better policy guidance to know what is expected of them, better technology, re-

sources, and training to navigate the ever-expanding flow of intelligence information. They also deserve our gratitude.

Thank you.

[The prepared statement of Mr. Winter follows:]

PREPARED STATEMENT OF DOUGLAS E. WINTER

SEPTEMBER 14, 2012

I first want to express, on behalf of Judge William H. Webster and my fellow Commissioners, our profound sympathy for the victims of the Fort Hood tragedy, their loved ones, families, and friends. Their loss is unimaginable. It is also America's loss.

I also want to acknowledge the honor and privilege of working with Judge Webster. He is one of America's most distinguished public servants—a former U.S. Navy officer, U.S. Attorney, U.S. District Judge, U.S. Circuit Judge, Director of the Federal Bureau of Investigation, and Director of the Central Intelligence Agency. He is also an inspiration, a mentor, and a friend.

In January 2010, Judge Webster asked me to join his independent investigation of the Federal Bureau of Investigation. At that time, we discussed the extraordinary scope of the Terms of Reference set out by FBI Director Robert S. Mueller III. We did not know then that our assignment would evolve and expand. We knew only the essential factual background, which I now describe.

BACKGROUND

On December 17, 2008, U.S. Army Major Nidal Malik Hasan visited the website of radical Islamic cleric Anwar Nasser al-Awlaki (sometimes spelled "Awlaki"). He sent a message to al-Awlaki. He sent another on January 1, 2009. The FBI Joint Terrorism Task Force (JTTF) in the San Diego Field Office, which led the FBI investigation of al-Awlaki, acquired the messages. An FBI Special Agent (SD–Agent) and Analyst (SD–Analyst) reviewed the messages. Concerned by the content of the first message and implications that the sender was a U.S. military officer, SD–Agent set leads to the JTTF in the Washington, DC, Field Office (WFO) and to FBI Headquarters on January 7, 2009.

Fifty days later, a WFO Supervisory Special Agent (WFO–SSA) read the lead and assigned it to a Defense Criminal Investigative Service (DCIS) Special Agent who served on the JTTF (WFO–TFO). Ninety days later, on May 27, 2009, WFO–TFO conducted an investigative assessment of Hasan, who worked as a psychiatrist at Walter Reed Army Medical Center. WFO–TFO queried certain FBI and Department of Defense (DoD) databases and reviewed the limited set of Army personnel records available to him. In the mean time, San Diego had acquired and reviewed 12 additional messages and emails from Hasan to al-Awlaki and two emails from al-Awlaki to Hasan. San Diego did not connect these communications to the lead.

WFO–TFO did not know about or review these additional communications. WFO's assessment concluded that Hasan was not "involved in terrorist activities." San Diego advised WFO that its assessment was "slim." Neither JTTF took further action. Hasan sent his last message to al-Awlaki on June 16, 2009. al-Awlaki did not respond.

In July 2009, the Army assigned Hasan to Fort Hood, Texas. In October 2009, the Army notified Hasan that he would be deployed to Afghanistan. On November 5, 2009, Hasan entered the Fort Hood deployment center carrying two handguns. He shouted "Allahu Akbar!"—Arabic for "God is great!"—and opened fire, killing 12 U.S. soldiers and one DoD employee, and injuring as many as 43 others.

This bare-bones summation veils an intricate and complex factual background.

The FBI conducted an internal investigation of how San Diego and WFO handled the Hasan-al-Awlaki communications. The FBI took specific steps to improve its ability to deter and detect threats like Hasan. Director Mueller determined that an additional, independent investigation of the FBI's actions was appropriate.

THE WEBSTER COMMISSION'S INVESTIGATION

Judge Webster's written statement provides the subcommittee with an overview of our lengthy and detailed investigation, our findings, and our recommendations as set forth in the *Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009.*

To fulfill Director Mueller's Terms of Reference, the Commission conducted inquiries into violent radicalization; the FBI's Joint Terrorism Task Force Program; the FBI's governing authorities; the FBI's information technology and document review infrastructure; the FBI's investigation of al-Awlaki; the FBI's assessment of Hasan; and the FBI's pre- and post-Fort Hood data holdings on Hasan.

Our analysis of the FBI's actions addressed knowledge and information sharing; ownership of the Hasan lead; WFO's assessment of Hasan; the FBI's information technology and review workflow; and training. Director Mueller also asked us to assess the FBI's remedial actions in the aftermath of the shootings, and to analyze whether the FBI's governing authorities strike an appropriate balance between protecting individual privacy rights and civil liberties and detecting and deterring threats such as that posed by Hasan. The investigation did not probe the shootings, which are the subject of a U.S. Army-led inquiry and military criminal proceeding against Hasan.

Director Mueller promised, and the FBI provided, full cooperation and support. No request was denied. No question went unanswered. The Commission had personal contact with more than 100 FBI Agents, Analysts, and Task Force Officers assigned to investigate al-Qaeda and other organizations linked with violent Islamic extremism. We spent many days in interviews, briefings, operational meetings, and conversations with personnel from at least 7 different Field Offices/JTTFs, FBI Headquarters, and the National Counterterrorism Center. We conducted a lengthy "no limits" field visit with a WFO counterterrorism unit of our choice that was not involved in the Hasan matter. We had direct access to the FBI's computer systems and to all personnel involved in the events at issue.

The Commission found shortcomings in FBI policy guidance, technology, information review protocols, and training. I summarize our analysis here. I caution the reader, however, against reaching conclusions based solely on this summary, which lacks the factual and analytical context of the *Final Report.* I also emphasize that we could not base our analysis on what we learned about Hasan or al-Awlaki on and after November 5, 2009. Our review was based on information known or available to the FBI at the time the actions were taken in the context of the FBI's then-existing policies and procedures, operational capabilities, and technological environment. Finally, we recognized our limited ability to predict what might have happened if different policies or procedures were in effect or personnel had made different decisions or taken different actions. We chose not to speculate. We examined instead the reasonableness of what did happen, in order to identify and recommend, when appropriate, better and corrective policies and procedures for the future.

ANALYSIS OF FBI ACTIONS

I. Knowledge and Information Sharing

A. The FBI's Understanding of Violent Radicalization

The FBI's understanding of violent radicalization is consistent with the contemporary views of the psychiatric community. Before the events at issue, the FBI had provided training on its radicalization model to Agents, Analysts, and Task Force Officers, including all personnel involved in the Hasan assessment. That training has expanded in the aftermath of the Fort Hood shootings.

B. The FBI's Knowledge About Anwar al-Awlaki

In early 2009, the FBI knew Anwar al-Awlaki as an English-speaking, anti-American, radical Islamic cleric and the subject of an FBI counterterrorism investigation. San Diego believed that al-Awlaki was developing ambitions beyond radicalization. WFO viewed him as merely inspirational. The FBI's full understanding of al-Awlaki's operational ambitions developed only after the attempted bombing of Northwest Airlines Flight 253 on Christmas day 2009.

C. The FBI's Knowledge About Nidal Malik Hasan

Our searches of the FBI's data holdings confirmed that San Diego's lead contained all of the FBI's actionable knowledge about Hasan as of January 7, 2009. The FBI's knowledge grew, or should have grown, over the next 5 months as San Diego acquired and reviewed 14 further messages from Hasan to al-Awlaki and two emails from al-Awlaki to Hasan. That knowledge also grew, or should have grown, as WFO conducted its assessment of Hasan on May 27, 2009, and San Diego reviewed that assessment in June 2009.

D. Information Sharing

The FBI did not share the Hasan information with any DoD employees other than DCIS and NCIS personnel assigned to the San Diego and WFO JTTFs.

Notice of the Hasan Assessment.—Prior to Fort Hood, FBI Field Offices informally shared information with DoD on a regular basis about counterterrorism assessments or investigations of members of the U.S. military, DoD civilian personnel, and others with known access to DoD facilities. However, there was no formal procedure or requirement to advise DoD about these assessments and investigations.

When San Diego set the lead to WFO, the FBI did not know whether the sender of the messages was a U.S. Army officer. In conducting its assessment of Hasan, WFO identified Hasan as a military officer but decided not to contact his chain of command. WFO's assessment concluded that Hasan was not involved in terrorist activities. Under these circumstances, the failure of either JTTF to advise DoD about the assessment was not unreasonable. However, the absence of a formal policy on notifying DoD of assessments or investigations of its personnel was unreasonable.

The Decision Not to Issue an Intelligence Information Report.—FBI policy is to share intelligence when dissemination has the potential to protect the United States against threats to National security or improve the effectiveness of law enforcement. San Diego decided not to issue an Intelligence Information Report (IIR) to DoD and other U.S. intelligence community members because of a mistake in interpreting Hasan's Defense Employee Interactive Data System (DEIDS) record. A DCIS Agent assigned to the San Diego JTTF (SD–TFO3) read the DEIDS abbreviation "Comm Officer" to mean "Communications Officer" rather than "Commissioned Officer." SD–Agent, who led the al-Awlaki investigation, thus believed that, if the sender was in fact Hasan, he might have access to IIRs. To protect the al-Awlaki investigation, he decided not to issue an IIR.

SD–TFO3's misinterpretation of the DEIDS record was understandable; others had made the same mistake. WFO's response to San Diego corrected this mistake and identified Hasan as an Army physician. Given WFO's identification of Hasan and its assessment that he was not involved in terrorist activities, San Diego had no reason to revisit the question of issuing an IIR.

II.Ownership of the Lead

The FBI's operational actions suffered from a lack of clear ownership of the Hasan lead. After setting the lead, San Diego believed that WFO was responsible for Hasan. WFO acted as if San Diego were responsible. The confusion resulted from the nature of Discretionary Action leads, a lack of policy guidance, the differing investigative interests of San Diego and WFO, a lack of priority, a misguided sense of professional courtesy, undue deference to military TFOs, and an inversion of the chain of command.

A. FBI Policy and Practice

In 2009, no FBI written policy established ownership of interoffice leads. In FBI practice, the receiving office was responsible for taking action in response to the lead and determining what, if any, additional investigative steps were warranted.

B. The Leads

San Diego's primary purpose in conducting the al-Awlaki investigation was to gather and, when appropriate, disseminate intelligence about him. The "trip wire" effect of the investigation in identifying other persons of potential interest was, in SD–Agent's words, a "fringe benefit."

SD–Agent set a Routine Discretionary Action lead to WFO and an Information-Only lead to FBI Headquarters that included Hasan's messages. The messages contained no suggestion of imminent violence and no overt threat. Because the lead did not demand action within 24 hours, FBI policy required SD–Agent to set a Routine lead. Because FBI practice was to give the receiving office discretion in assessing potential threats in its Area of Responsibility, the lead was "[f]or action as deemed appropriate."

The decision to set a Routine Discretionary Action lead was reasonable under the circumstances and existing policies. The follow-up, however, was not adequate.

C. The Response

San Diego set the lead on January 7, 2009. At that time, there was no formal policy guidance on the assignment or resolution of Routine leads. The timing of assignments depended on the practice of the receiving supervisor.

At WFO, the receiving Supervisory Special Agent (WFO–SSA) did not read and assign the lead until February 25, 2009, nearly 50 days after the lead was set.

No formal FBI policy set a deadline for the completion of work on Routine leads. Because file reviews occur on a quarterly basis, informal FBI policy required personnel to complete work on Routine leads within 90 days of assignment.

WFO–SSA assigned the lead to a DCIS Agent detailed to the JTTF (WFO–TFO). WFO–TFO waited 90 days—until May 27, 2009, the day his work on the lead was

supposed to be completed—to read it and take action. The 90-day delay in even reading the lead, let alone taking action, was unreasonable. That delay may have affected the shape, scope, and outcome of WFO's assessment of Hasan, which took place in 4 hours on that 90th day.

Five months passed before WFO responded to San Diego's lead. The delay pushed Hasan further from the minds of SD–Agent and SD–Analyst, and may have contributed to their failure to connect other Hasan communications with the lead.

D. The Impasse

Although the lead identified a potential threat in the Washington, DC, area, WFO–SSA and WFO–TFO treated Hasan as part of San Diego's investigation of al-Awlaki. This perspective appears to inform their apprehension about interviewing Hasan and conducting a more expansive assessment without first checking with San Diego. Yet WFO declined to take further action even after San Diego criticized the assessment as "slim," and instead offered to "re-assess" if San Diego, "request[ed] any specific action."

E. Deference to Military Task Force Officers

SD–Agent engaged DCIS and NCIS Task Force Officers (TFOs) in San Diego in researching Hasan's military status and deciding whether to circulate an IIR. Those actions were reasonable and prudent. Interagency synergy is a prime reason for the JTTF Program.

That synergy weakens, however, when TFOs assume sole responsibility for investigating members of their own departments or agencies. WFO–SSA's assignment of the lead to WFO–TFO had practical advantages. As a DCIS Agent, WFO–TFO had access to DoD resources and databases that were not available to the FBI. He also had an insider's knowledge of DoD practices and procedures that could prove vital to an assessment of a service member. However, he also brought the subjectivity of an insider to the assessment. That subjectivity may have caused undue deference to the Army chain of command and undue concern about the potential impact of an interview on Hasan's military career, which appear to have driven the decision not to interview Hasan or contact his superiors.

F. An Inverted Chain of Command

The JTTF synergy also weakens when the FBI looks to TFOs to resolve disputes between offices. Here, after SD–Agent reviewed WFO's response to the lead, he asked SD–TFO3 to contact WFO–TFO, DCIS Agent to DCIS Agent.

SD–Agent should have called WFO–SSA. If they could not resolve matters, SD–Agent should have raised the dispute up the FBI chain of command to his supervisor, who could have reviewed the matter and contacted WFO–SSA's supervisor. If disagreement continued, the supervisors could have turned to FBI Headquarters for resolution. This is how the FBI has routinely handled interoffice disputes and disagreements, but only as a matter of unofficial policy.

G. The Lack of Formal Policies

The lack of formal policy guidance defining ownership of this lead and requiring elevation of interoffice disputes caused or contributed to a situation in which two JTTFs effectively disowned responsibility for the lead—each believing that the other office was responsible. That belief affected, in turn, each JTTF's sense of priority when it came to the assessment, the search for additional Hasan-al-Awlaki communications, and how the conflict between the offices should be resolved.

III. The Assessment

WFO–SSA and WFO–TFO erred in the process they followed to conclude that Hasan's communications with al-Awlaki were benign and acceptable. They also erred in failing to search the database in which electronic communications were stored, if only to determine whether al-Awlaki had replied to Hasan's messages. Their assessment of Hasan was belated, incomplete, and rushed, primarily because of their workload; the lack of formal policy setting deadlines for the assignment and completion of Routine counterterrorism assessments; WFO–TFO's lack of knowledge about and training on DWS–EDMS; the limited DoD personnel records available to WFO–TFO and other DoD TFOs; and the delay in assigning and working on the lead, which placed artificial time constraints on the assessment.

A. The Records Check

WFO–TFO assessed Hasan using the limited Army Electronic Personnel File that WFO–TFO had authority to access. Those records praised Hasan's research on Islam and the impact of beliefs and culture on military service, and showed that he held a security clearance and had been promoted to Major weeks earlier. WFO–

TFO thus believed—and WFO–SSA agreed—that the Army encouraged Hasan's research and would approve of his communications with al-Awlaki.

Based on this simple records check, those conclusions may have been reasonable. Hasan's two messages solicited Islamic opinions. He made no attempt to disguise his identity and used an email address that revealed his proper name.

The Army records available to WFO–TFO did not present a complete or accurate picture of Hasan. Indeed, their contents were misleading. WFO–TFO—and, in turn, the FBI—did not have access to the disturbing contents of Hasan's personal files at Walter Reed Army Medical Center and the Uniformed Services University of Health Sciences.

Despite the Army's interest in Hasan's research, his communications with an inspirational and potentially operational radicalizer under FBI investigation deserved scrutiny beyond a simple records check. Regardless of the contents of his Electronic Personnel File, the lead warranted a closer look at Hasan.

B. The Decision Not to Interview Hasan

The decision not to interview Hasan was flawed. WFO–TFO and WFO–SSA believed that an interview could jeopardize the al-Awlaki investigation by revealing the FBI's access to Hasan's messages. This explanation is not persuasive. FBI Agents talk to subjects and assess threat levels every day without explaining the source of their knowledge.

WFO–TFO and WFO–SSA also concluded, from the records check, that Hasan was not "involved in terrorist activities." As a result, they believed that an interview and contact with Hasan's chain of command might jeopardize his military career, contrary to the FBI's "least intrusive means" requirement. Under that requirement, an investigative technique (for example, a records check or interview) may be used if it is the least intrusive feasible means of securing the desired information in a manner that provides confidence in the information's accuracy.

The fact that messages to a radical imam appear to be benign academic inquiries does not answer the question of whether Hasan was a threat. The "least intrusive means" requirement did not prohibit further inquiry into that question, but would require a careful balancing of the competing interests of assessing a potential threat and minimizing potential harm to the subject of the assessment.

Moreover, when San Diego expressed doubts about WFO's assessment, the calculus of the least intrusive means requirement should have changed. The next-least intrusive means (for example, an interview) could have been used to resolve any doubts about the messages and provide more confidence in the accuracy of the information supporting WFO's conclusion.

C. The Failure to Search for Additional Messages

WFO–TFO did not even know that DWS–EDMS, the database in which the Hasan-al-Awlaki communications were stored, existed until after the Fort Hood shootings. As a result, WFO–TFO searched only databases known to him and did not find any of the later messages. After receiving WFO's assessment, which stated incorrectly that WFO had searched all FBI databases, San Diego did not search DWS–EDMS for additional messages acquired during the intervening 5 months.

The failure to search for additional messages appears to have had significant ramifications. That search, if performed on May 27, 2009, the date of WFO's assessment, would have returned 12 additional communications from Hasan and al-Awlaki's two emails to Hasan. Although none of the messages contained a suggestion of imminent violence or an overt threat, the additional messages could have undermined the assumption that Hasan had contacted al-Awlaki simply to research Islam.

The failure to search for additional messages resulted primarily from the FBI's failure to provide TFOs with training on DWS–EDMS and other FBI databases, the search and information management limitations of DWS–EDMS, the lack of ownership of the Hasan lead, the lack (at that time) of a baseline collection plan, and the absence of the type of initiative that Agents, Analysis, and TFOs should be encouraged to take, particularly when confronted with dissonant information or an interoffice dispute.

D. Workload and the Lack of Formal Policies

The nearly 50-day delay in the assignment of the lead and the 90-day delay in taking action on the lead suggest that WFO–SSA and WFO–TFO were overburdened. That underscores the importance of formal policy direction that allows personnel to understand, prioritize, and manage their workloads.

The absence of formal policy guidance setting deadlines for assignment and resolution of Routine counterterrorism leads and establishing a baseline for information

to be collected in counterterrorism assessments caused or contributed to an assessment of Hasan that was belated, incomplete, and rushed.

IV. Information Technology and Review

A crucial lesson of Fort Hood is that the information age presents new and complex counterterrorism challenges for the FBI. Diverse and ever-growing waves of electronic information confront its law enforcement and intelligence-gathering activities. Emerging technologies demand changes in the ways that the FBI acquires, stores, reviews, organizes, manages, disseminates, and acts on intelligence.

The actions of the Agents, Analysts, and Task Force Officers who handled the Hasan information cannot be judged fairly or accurately without an understanding of their working environment—and, in particular, their technological environment. Our investigation revealed that the FBI's information technology and review protocols were, then and now, less than adequate for fulfilling the FBI's role as the premier U.S. intelligence and law enforcement agency combating domestic terror.

A. Information Technology Limitations

DWS–EDMS, the primary database under review, is a capable tool that lacks the modern hardware infrastructure needed to fulfill and preserve its crucial functionality. The relatively aged server configuration for DWS–EDMS and its ever-increasing data storage demands, coupled with ever-increasing use, create issues that we witnessed in our hands-on use of the system. DWS–EDMS also lacks a "live" or "failover" disaster recovery backup.

B. Information Review Workflow

In examining San Diego's review of the information acquired in the al-Awlaki investigation, we identified serious concerns about the available technology and two interrelated concerns about human actions: Questionable decisions in reviewing certain communications and the failure to relate subsequent messages to the lead.

The DWS–EDMS collection presented, in SD–Analyst's words, a "crushing volume" of information. We were unable to assess the reasonableness of San Diego's review decisions and tracking of messages outside the context of the nearly 20,000 other al-Awlaki-related electronic documents that SD–Agent and SD–Analyst reviewed prior to Hasan's final message on June 16, 2009.

We found, however, that the FBI's information technology and document review workflow did not assure that all information would be identified and managed correctly and effectively in DWS–EDMS because of a confluence of factors: (1) The humanity of the reviewers; (2) the nature of language; (3) the "crushing volume" of the al-Awlaki information; (4) the workload; (5) limited training on the databases and search and management tools; (6) antiquated and slow computer technology and infrastructure; (7) inadequate data management tools; (8) the inability to relate DWS–EDMS data easily, if at all, to data in other FBI stores; and (9) the absence of a managed quality control regime for review of strategic collections.

The *Final Report* discusses each of these factors in detail (see Chapters 4–6 and 11). The confluence of these diverse human and technological factors forced SD–Agent and SD–Analyst to review, using a linear, forward-looking workflow, each of the Hasan-al-Awlaki communications in isolation as 18 of the nearly 8,000 electronic documents that they reviewed between December 18, 2008, and June 16, 2009, the dates of Hasan's first and last messages to al-Awlaki. That workflow encouraged anticipatory review, analysis, and identification of products, but discouraged reflection, connectivity, and retrospective review and analysis. The operational and technological context in which SD–Agent and SD–Analyst worked, not their actions as reviewers, was unreasonable.

C. Data Aggregation

FBI Agents, Analysts, and Task Force Officers regularly consult many databases in the performance of their duties. In 2009, with few exceptions, users accessed each database using a discrete interface, password, and search engine. Our investigation found that planning for enterprise data aggregation, and consolidating and conforming the contents of these diverse databases, are vital to the FBI's ability to respond to the threat of terrorism.

ASSESSMENT OF FBI REMEDIAL ACTIONS

At Director Mueller's request, Part Three of the Final Report assessed the changes to FBI policies, operations, and technology that resulted from its own internal review and subsequent events. We applaud these steps, which are outlined in Exhibit B.

ANALYSIS OF THE FBI'S GOVERNING AUTHORITIES

A. Existing Authorities

After an extensive review of the FBI's governing authorities (see Chapter 3), we asked representatives of Congressional oversight staff (the Majority and Minority staffs of the Senate and House Judiciary and Intelligence Committees) and public interest groups (the American Civil Liberties Union and the American Enterprise Institute) to identify their concerns abut the impact of the governing authorities on privacy rights and civil liberties.

Part Four of the *Final Report* assesses those concerns. We concluded that existing authorities balance the FBI's responsibility to detect and deter terrorism with protection of individual privacy rights and civil liberties. We believe, however, that the FBI should monitor and report on its use of investigative techniques that raise concern through the Office of Inspection and Compliance, Inspection Division, and National Security Division. The FBI should modify or abandon policies and protocols that prove unacceptably harmful to privacy rights or civil liberties.

B. Additional Authorities

We interviewed a broad range of FBI personnel involved in counterterrorism work; former FBI and other U.S. intelligence community personnel; and members of the Majority and Minority staff of the Congressional Judiciary and Intelligence Committees. Although we received a number of recommendations, we identified, but took no position on, two legislative actions that the FBI could propose to improve its ability to deter and detect terrorist threats.

The Communications Assistance for Law Enforcement Act.—The FBI believes that amending the Communications Assistance for Law Enforcement Act (CALEA) (1994), 47 U.S.C. § 1001 et seq., is an immediate priority. Congress enacted CALEA to assure that law enforcement obtains prompt and effective access to communications services when conducting a lawful electronic surveillance. The statute recognizes that surveillance may be difficult, if not impossible, absent an existing level of capability and capacity on the part of communications service providers. The threat to our National security—increasingly explicit in FBI investigations—is that service providers using new technologies often lack that capability and capacity.

Administrative Subpoena Authority.—The FBI's counterterrorism authorities are not as robust, definitive, and consistent as its law enforcement authorities. The FBI has the authority to issue administrative subpoenas in narcotics, child-abuse, and child-exploitation investigations, but not in counterterrorism investigations. This inconsistency is noteworthy, although we recognize that counterterrorism investigations may implicate potential risks to civil liberties and privacy interests in ways that traditional law enforcement investigations do not.

RECOMMENDATIONS

We made 18 formal recommendations for corrective and enhancing measures on matters ranging from FBI policies and operations to information systems infrastructure, review protocols, and training. Exhibit A summarizes those recommendations. We also assessed whether any administrative action should be taken against any employee involved in this matter, and we concluded that administrative action was not appropriate.

We recognize that the FBI has continued to evolve as an intelligence and law enforcement agency in the aftermath of Fort Hood and in furtherance of internal and external recommendations that followed, including the Special Report of the Senate Committee on Homeland Security and Governmental Affairs (February 3, 2011). To the extent our Recommendations may parallel or implicate actions and initiatives proposed internally or by others, they should not be read to suggest that the FBI has not been diligent in pursuing those actions and initiatives, but to underscore their importance.

CONCLUSION

In the words of our *Final Report:* "We conclude that, working in the context of the FBI's governing authorities and policies, operational capabilities, and the technological environment of the time, FBI and Joint Terrorism Task Force personnel who handled relevant counterterrorism intelligence information made mistakes. We do not find, and do not suggest, that these mistakes resulted from intentional misconduct or the disregard of duties. Indeed, we find that each Special Agent, Intelligence Analyst, and Task Force Officer who handled the [intelligence] information acted with good intent. We do not find, and do not believe, that anyone is solely responsible for mistakes in handling the information. We do not believe it would be

fair to hold these dedicated personnel, who work in a context of constant threats and limited resources, responsible for the tragedy at Fort Hood." We concluded instead that "these individuals need better policy guidance to know what is expected of them in performing their duties, and better technology, review protocols, and training to navigate the ever-expanding flow of intelligence information." We also concluded that the FBI should continue to focus on compliance monitoring and the oversight of authorized investigative techniques that may affect privacy rights and civil liberties.

EXHIBIT A

SUMMARY OF WEBSTER COMMISSION RECOMMENDATIONS

Policies

A.1: A Formal Policy on Counterterrorism Command-and-Control Hierarchy
A.2: A Formal Policy on the Ownership of Counterterrorism Leads
A.3: A Formal Policy on Elevated Review of Interoffice Disagreements in Counterterrorism Contexts
A.4: A Formal Policy on the Assignment and Completion of Routine Counterterrorism Leads
A.5: A Formal Policy on Counterterrorism Leads Assigned to JTTF Task Force Officers
A.6: A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessments and Investigation of Law Enforcement Personnel
A.7: A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessment and Investigation of Other Government Personnel

Operations

B.1: Continued Integration of Intelligence Analysts into Operations

Information Technology and Review

C.1: Expedite Enterprise Data Management Projects
C.2: Expand and Enhance the Data Integration and Visualization System
C.3: Acquire Modern and Expanded Hardware for DWS–EDMS
C.4: Acquire Advanced Information Search, Filtering, Retrieval, and Management Technologies
C.5: Adopt Managed Information Review Protocols for Strategic Collections and OtherLarge-Scale Data Collections

Governing Authorities

D.1: Increase Office of Integrity and Compliance (OIC) and Inspection Division Compliance Reviews and Audits
D.2: Assure Strict Adherence to Policies That Ensure Security for Information That Lacks Current Investigative Value
D.3: The FBI's National Security letter, Section 215 Business Record, Roving Wiretap, and "Lone Wolf" Authorities Should Remain in Effect
D.4: Update Attorney General Guidelines Affecting Extra-Territorial Operations

Training

E.1: Train Task Force Officers on FBI Databases Before They Join Joint Terrorism Task Forces

EXHIBIT B

SUMMARY OF FBI REMEDIAL ACTIONS

Information Sharing

(1) FBI–DoD Clearinghouse Process for Counterterrorism Assessments and Investigations of Military Personnel
(2) Consolidation of FBI–DoD Memoranda of Understanding on Information Sharing, Operational Coordination, and Investigative Responsibilities

Operations

(1) Discontinuance of "Discretionary Action Leads"
(2) Counterterrorism Baseline Collection Plan
(3) Triggers for Assessments/Investigations
(4) Decisions to Close Certain Investigations of DoD Personnel
(5) Identification and Designation of Strategic Collections

Technology

(1) Automatic Linking of Email Data
(2) Automatic Flagging of Certain Email Data
(3) Flagging DWS–EDMS Activity Across Cases
(4) Workload Reduction Tools
(5) DWS–EDMS September 2011 Release

Training

(1) Virtual Academy
(2) Classroom Training
(3) Database Training

THE WILLIAM H. WEBSTER COMMISSION ON THE FEDERAL BUREAU OF INVESTIGATION, COUNTERTERRORISM INTELLIGENCE, AND THE EVENTS AT FORT HOOD, TEXAS, ON NOVEMBER 5, 2009

The Honorable William H. Webster, Chair

COMMISSIONERS

Douglas E. Winter, (BRYAN CAVE LLP), Deputy Chair and Editor-in-Chief
Adrian L. Steel, Jr., (MAYER BROWN LLP), Governing Authorities Liaison
William M. Baker, (former FBI Assistant Director, CRIMINAL INVESTIGATIVE DIVISION)
Russell J. Bruemmer, (WILMER HALE)
Kenneth L. Wainstein, (CADWALADER, WICKERSHAM & TAFT LLP)

ADJUTANT

Stephen J. Cox, (APACHE CORPORATION)

ASSOCIATES

George F. Murphy, (BRYAN CAVE LLP)
Margaret-Rose Sales, (MAYER BROWN LLP)

Mr. MCCAUL. Thank you, Mr. Winter.

The Chairman now recognizes Professor Manji for her testimony.

STATEMENT OF ISHRAD MANJI, DIRECTOR, MORAL COURAGE PROJECT, NEW YORK UNIVERSITY

Ms. MANJI. Thank you.

Good morning. My name is Irshad Manji, and I am here in my capacity as founder and director of the Moral Courage Project.

Before I formally begin, allow me also to express my sympathy to those, both American and not, who have been victimized by this week's violence in Libya, Egypt, and now Yemen.

Housed in the Wagner School of Public Service, the Moral Courage Project teaches people worldwide to speak up when others, frankly, want to shut them up. We are motivated not just to break silences but also to combat the abuse of power, in other words the corruption, that comes from the fear of speaking out. This means understanding why silences develop in the first place, which brings me to the question that concerns our hearing.

Let me be clear: I do not know if one or more FBI officers intentionally withheld information about Major Nidal Malik Hasan. But personal experiences leave me skeptical about whether the standard bearers of National security are willing to share vital information, whether with the public or with each other.

I will give you a couple of examples in a moment. First, let me address why I would have personal experiences on this front. The reason is I am a devoted Muslim who loves God; and, because I

love God, I speak up whenever anybody uses Islam to violate all of our God-given liberties and human rights.

As refugees from East Africa, my family and I settled on the West Coast of Canada; and there I grew up attending two types of schools, the multi-racial, multi-faith public school, and then every Saturday, for several hours at a stretch, the Islamic religious school, the madrassa.

At madrassa, I asked candid questions. For instance, why can't Muslims take Jews and Christians as friends? At the age of 14, having asked one too many of these questions, I got booted out of the madrassa. But as I have had to assure my mortified mother more than once, leaving madrassa does not mean leaving Allah.

I decided to study Islam on my own and discovered that there is an Islamic tradition of questioning, of reinterpreting, and even of dissenting with the clerics. It is this tradition that empowers me to reconcile my faith with freedom. All of which puts me and my team on the receiving end of death threats and actual violence not just in Muslim-majority countries but also in this part of the world. That is why I have first-hand experience with some of the inner workings of National security. That is how I have come to observe the censorship that plagues many good people, people to whom we do owe gratitude and whose mission is to protect the public.

In my remaining time, I would like to share two stories. Although the first takes place in Canada, of which I remain a citizen, it foreshadows the second story, which takes place in the United States, where I now live and work.

In June, 2006, Canadian police arrested young Muslims for plotting to blow up Parliament and behead the Prime Minister. The Toronto 17, as they came to be known, called their campaign Operation Badr, B-a-d-r, Badr. Operation Badr is a tribute to the battle of Badr, the first decisive military victory by Prophet Mohammed.

Now, police knew that religious symbolism helped inspire the Toronto 17. Still, at the press briefing to announce those arrests, police did not mention the words Muslim or Islam.

At their second meeting with the press, police boasted, bragged about avoiding the words Muslim and Islam, again despite knowing that Operation Badr had been organized in the name of Islam.

Three months later, at a police conference, I raised my concern about the silence. After my plea for honesty, several law enforcement insiders, independent of each other, confided to me that the lawyers prevented these authorities from publicly uttering the words Muslim and Islam.

As for my experiences in the United States, here is a concrete one. In 2009, I received media calls about David Headley, a U.S. citizen who helped plan the terrorist attacks on Bombay in 2008, in other words, the year before. Apparently, Mr. Headley had named me among his targets, too. Journalists wanted to know how that made me feel. You can guess my response.

What made me feel worse, though, was that these media calls came in a full day before any National security officials got in touch. Somehow, somewhere their chain of communication had broken down.

The research on institutional silos and silence suggests multiple forces at play. But the antidote to all of these forces is moral cour-

age, the willingness to speak up when others want to shut you down.

I thank you for this invitation and, unlike my madrassa teacher, I welcome your questions.

[The prepared statement of Ms. Manji follows:]

PREPARED STATEMENT OF IRSHAD MANJI

SEPTEMBER 14, 2012

My name is Irshad Manji. I am here in my capacity as founder and director of the Moral Courage Project at New York University.

Housed in the Wagner School of Public Service, the Moral Courage Project teaches people worldwide to speak up when others want to shut them up. We are motivated not just to break silences, but also to combat the abuse of power—the corruption—that comes from the fear of speaking out.

This means understanding why silences develop in the first place, which brings me to the question that concerns our hearing.

Let me be clear: I do not know if one or more FBI officers intentionally withheld information about Major Nidal Malik Hasan. But personal experiences leave me skeptical about whether the standard-bearers of National security are willing to share vital information, whether with the public or with each other.

I will give you a couple of examples in a moment. First, allow me to address why I would have personal experiences on this front. The reason is: I am a devoted Muslim who loves God, and because I love God, I speak up whenever Muslims use Islam to violate our God-given liberty and human rights.

As refugees from East Africa, my family and I settled on the West Coast of Canada. There, I grew up attending two types of schools—the multi-racial, multi-faith public school and then, every Saturday, for several hours at a stretch, the Islamic religious school (madressa). At madressa, I asked candid questions. For instance, why can't Muslims take Jews and Christians as friends?

At the age of 14, having asked one too many of these questions, I got booted out of madressa. But as I had to assure my mortified mother—more than once—leaving madressa does not mean leaving Allah.

I decided to study Islam on my own, and discovered that there is an Islamic tradition of questioning, re-interpreting, and even dissenting with the clerics. It is this tradition that empowers me to reconcile my faith with freedom.

All of which puts me and my team on the receiving end of death threats—and actual violence—not just in Muslim-majority countries, but also in this part of the world. That is why I have first-hand experience with some of the inner workings of National security.

And that is how I have come to observe the censorship that plagues many good people whose mission is to protect the public.

In my remaining time, I would like to share two stories. Although the first takes place in Canada, of which I remain a citizen, it foreshadows the second story, which takes place in the United States, where I now work and live.

In June 2006, Canadian police arrested young Muslims for plotting to blow up Parliament and behead the Prime Minister. The "Toronto 17," as they came to be known, called their campaign, Operation Badr. This title is a tribute to the Battle of Badr, the first decisive military victory by Prophet Muhammad.

Police knew that religious symbolism helped inspire the Toronto 17. Still, at the press briefing to announce those arrests, police did not mention the words "Muslim" or "Islam."

At their second meeting with the press, police boasted about avoiding the words "Muslim" and "Islam"—again, despite knowing that Operation Badr had been organized in the name of Islam.

Three months later, at a police conference, I raised my concern about this silence. After my plea for honesty, several law enforcement insiders, independent of each other, confided to me that lawyers prevented authorities from publicly uttering the words "Muslim" and "Islam."

As for my experiences in the United States, here is a concrete one: In 2009, I received media calls about David Headley, a U.S. citizen who helped plan the terrorist attacks on Bombay the year before. Apparently, Mr. Headley had named me among his targets. Journalists wanted to know how that made me feel. You can guess my response.

What made me feel worse was that these media calls came in a full day before any National security officials got in touch. Somehow, somewhere, their chain of communication had broken down.

The research on institutional silos—and silence—suggests multiple forces at play. But the antidote to all of these forces is moral courage: The willingness to speak up when others want to shut you up.

I thank you for this invitation and, unlike my madressa teacher, I welcome your questions.

Mr. MCCAUL. Thank you, Professor, and we appreciate your courage. Thank you for being here.

The Chairman now recognizes Mr. Leiter.

STATEMENT OF MICHAEL E. LEITER, FORMER DIRECTOR OF THE NATIONAL COUNTERTERRORISM CENTER

Mr. LEITER. Mr. Chairman, Mr. Ranking Member, it is a pleasure to be back. This is my first appearance before the Congress outside of the Executive branch, and I have to say the freedom is rather invigorating.

Today, I am actually appearing as a member of the Homeland Security Project at the Bipartisan Policy Center. That is the follow-on organization to the 9/11 Commission, led which the very distinguished and talented Governor Tom Kean and Congressman Lee Hamilton. Although, of course, also my comments are really based on my time, over 4 years, as the head of the National Counterterrorism Center, as well as serving in the Navy and the Department of Justice.

Now, rather than spending my 5 minutes now going over extensively where I think improvements have been made, I would like to focus most of my comments on where I think there are still challenges that the Congress and the Executive branch faces over the next several years. But I do want to highlight, because you are focused on a failure—Congressman McCaul, you obviously noted the successes, and there really have been many, and many of these successes we simply take for granted today: The fact that we have a single, consolidated watch list at the National Counterterrorism Center; the fact that we have analysts and information systems from a variety of organizations all in one place; the fact that we have 104 Joint Terrorism Task Forces and fusion centers.

These are all—none of this is to say that the problems are solved, but this is to say that the improvements are quite tremendous. The tragedy of the 13 brave Americans who were lost at Fort Hood can never be eliminated.

All that being said, that we have avoided large-scale terrorist attacks in the United States and a total of 14 individuals have been killed in the United States in the past 11 years is, in my view, nothing short of remarkable. Tragic that every one of those lives was lost but a record which I do think that the Congress and the U.S. Government and our allies can in fact be proud of.

Now, having accepted that not everything is right, I would offer two caveats before I go into the areas where I think they can be improved.

First, I think the Congress and the Executive branch must be very careful not to conflate all information-sharing problems as being the same. There is real sophistication in this. What happened on Christmas day, an intelligence failure, was one type of informa-

tion challenge; and it is a very different challenge from what happened at Fort Hood. I say that because I think it is important to, as I say, get under the hood, examine these with some specificity.

Second, I think this committee knows this well, but we have to continue to remember that information sharing is not always unmitigated good. We need look no father than WikiLeaks to remember that, as we share information, we must also do it in a way that not only protects privacy and civil liberties but protects the security of that information.

I believe these two things can be reconciled, but we cannot forget that there are dangers as well.

Very quickly, where do I see some opportunities and need for improvement? I will divide it into five basic areas: Legal, policy, budgetary, personnel, and technology.

First, on the legal front, I am a recovered lawyer, but I will say there is probably no area in which I work in National security where the legal landscape is a myriad of complicated, conflicting statutes, and it is extremely difficult to ever know how information can or cannot be shared. The burden that that puts on operators and analysts, not to mention lawyers, is tremendous.

Although I think the Foreign Intelligence Surveillance Act, FISA, serves some very valuable purposes both for collection and for protection of civil liberties, anything that Congress can do to simplify that law, especially in an era of rapidly-changing technology, would be critically important.

Second, on the policy front, I think it is important that the Congress and the Executive branch work together to move legal policies—pardon me, move information-sharing policies in a far more rapid way than they move today. I think as a general matter—and I say this having served in a Republican and Democratic administration. I think as a general matter administrations have gotten these policies right about how information should be shared, but the pace at which these discussions occur borders on the Biblical. In an era of rapidly-evolving terrorist threats we cannot allow these discussions to go on endlessly. The Congress must demand that the Executive branch rapidly adopt policies, like the Attorney General guidelines, to ensure there is effective information sharing once laws are passed.

On the budgetary front, this committee knows quite well the pressures that all of National security and State and local governments will face in the coming years. We have spent an enormous amount of money building Joint Terrorism Task Forces and State and local fusion centers. In my view, although these have done quite well, as we enter a more austere budgetary period the Congress will have to look quite closely at how we can rationalize and truly create a National system and not simply a patchwork of entities.

Very quickly on the last two points, personnel and technology, I think part of the failure at Fort Hood was undoubtedly a thorough understanding among some well-intentioned agents and officers about what were signs and symptoms of radicalization in the population. This sort of training must be continued; and, of course, training on the tools that people already have must be increased.

Last, but not least, technology can help us here. We all know that technology is not a panacea. But basic technological tools which flag information for people allow uncorrelated information to be shown to a variety of individuals, information to be shared across security regimes amongst the FBI, National Counterterrorism, Department of Defense, and the like are absolutely critical. So it is not simply two agents looking at an email trying to decide whether or not an individual is radicalized, but we are actually taking full advantage of the larger National security community. Technology exists to do that today.

With that, Mr. Chairman, I welcome your questions. It is very good to be back. I want to simply close on joining you on your notes of condolences for the loss that we saw in Libya, the losses that we see every day in Afghanistan, and the losses that we suffered in Fort Hood.

[The prepared statement of Mr. Leiter follows:]

PREPARED STATEMENT OF MICHAEL E. LEITER

SEPTEMBER 14, 2012

INTRODUCTION

Mr. Chairman, Mr. Ranking Member, Members of the subcommittee: I am pleased to have the opportunity to appear before you today. This subcommittee has been at the center of ensuring that needed reform is taking place in our Government. I am deeply grateful to you for your sustained leadership in that effort. The subject of today's hearing, "Lessons from Fort Hood: Why Can't We Connect the Dots to Protect the Homeland?" is of critical importance to National security.

Today, I appear in my capacity as a Task Force Member of the Bipartisan Policy Center's Homeland Security Project, a successor to the 9/11 Commission. Drawing on a strong roster of National security professionals, the HSP works as an independent, bipartisan group to monitor the implementation of the 9/11 Commission's recommendations and address other emerging National security issues.

HSP includes the following membership:

- Governor Thomas H. Kean, Former Governor of New Jersey; Chairman of the 9/11 Commission; and Co-Chair of the Homeland Security Project;
- The Honorable Lee H. Hamilton, Former Congressman from Indiana; Vice-Chair of the 9/11 Commission; and Co-Chair of the Homeland Security Project;
- Peter Bergen, Director, National Security Studies Program at the New America Foundation;
- Christopher Carney, Former Congressman from Pennsylvania and Chair of the U.S. House Homeland Security Oversight Committee;
- Stephen E. Flynn, Ph.D., Founding Co-Director of the George J. Kostas Research Institute for Homeland Security and Professor of Political Science at Northeastern University;
- Dr. John Gannon, Former Deputy Director of the CIA for Intelligence;
- Dan Glickman, Senior Fellow, Former Secretary of Agriculture; Former Chairman of the U.S. House Intelligence Committee;
- Dr. Bruce Hoffman, Director, Center for Peace and Security Studies, Georgetown University;
- Michael P. Jackson, Chairman and CEO, VidSys, Inc. and Former Deputy Secretary of the U.S. Department of Homeland Security;
- Ellen Laipson, President and CEO of the Stimson Center and member of the President's Intelligence Advisory Board;
- Michael E. Leiter, Senior Counselor to the Chief Executive Officer, Palantir Technologies and Former Director of the National Counterterrorism Center;
- Edwin Meese III, Former U.S. Attorney General, Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation;
- Erroll G. Southers, Former Chief of Homeland Security and Intelligence for the Los Angeles Airports Police Department; and Associate Director of the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California;

- Richard L. Thornburgh, Former U.S. Attorney General and Governor of Pennsylvania;
- Frances Townsend, Former Homeland Security Advisor and Deputy National Security Advisor for Combating Terrorism;
- Jim Turner, Former Congressman from Texas and Ranking Member of the U.S. House Homeland Security Committee.

My HSP colleagues and I believe the depth of this group's experience on National security issues can be of assistance to you and the Executive branch and we look forward to continuing to work with you.

I will also draw on my experience as former Director of the National Counterterrorist Center (NCTC), a post I stepped down from 1 year ago. While I will address certain aspects of deficiencies in information sharing surrounding the Fort Hood shootings, I believe I can best help the subcommittee by sharing my views about how well the Government is sharing information generally. While my testimony is in part based on my work with the HSP, it does not necessarily reflect the views of my HSP Board Member colleagues.

Now, exactly 11 years after the tragic 9/11 attacks, and 8 years since *The 9/11 Commission Report,* is an appropriate time to take stock of how well our Government is sharing information.

OVERVIEW

The 9/11 Commission documented major failures of National security-related agencies to share vital terrorist-related information in the months and years before the 9/11 attacks. In the pre-9/11 period, legal, policy, and cultural barriers among agencies created serious impediments to information sharing. The Commission made a number of specific recommendations to improve information sharing across our Government and regarded it imperative that all levels of Government make improvements.

Information sharing within the Federal Government, and among Federal, State, local, and Tribal authorities, and with allies, while not perfect, has been considerably improved since 9/11. The level of cooperation among all levels of government is higher than ever. State and local officials have a far greater understanding not only of the threat and how to respond to it but also of their communities and those who may be at risk of radicalization. The formation of the National Counterterrorism Center (NCTC) was a major step toward improved information sharing. When the follow-on organization to the Commission issued grades and reviews in late 2005 and subsequently, it cited the creation of NCTC and its performance as a success in National security reform. Although I am admittedly biased on this point, I certainly agree that NCTC has played and continues to play a critical information-sharing role.

NCTC's information-sharing responsibilities are extremely broad and encompass items that many now take as a given—even though 10 years ago they were nonexistent. For example, NCTC's maintenance of a consolidated watch list that is available to local police during a car stop, foreign service officers checking a visa application, and homeland security professionals at a border, ensure that a critical information-sharing gap from 9/11 is filled. Similarly, NCTC's three-times daily video conferences ensure that every element of the U.S. Government knows what threats are on the radar. In addition the presence of analysts from more than 20 organizations at NCTC, sitting side-by-side, and sharing information countless times a day is a radical (and positive) shift from 2001. Finally, the Interagency Threat Assessment and Coordination Group (ITACG) provides greater information sharing between State and local officials and the whole of the U.S. Counterterrorism Community. In short, when it comes to information sharing the U.S. Government has moved forward in leaps and bounds.

This improvement is, of course, not just because of NCTC but because of an equally concerted effort by the FBI, DHS, and others. Most notably there are now 104 Joint Terrorism Task Forces throughout the Nation, and 72 Fusion Centers in which Federal, State, local, and Tribal authorities investigate terrorism leads and share information. Since 2004, DHS has provided more than $340 million in funding to the Fusion Centers. Information sharing with the private sector has also become routine and is an important part of our defenses.

Despite these improvements, there is no doubt that weaknesses exist—although I frankly believe we must be careful not to equate more recent information-sharing failures with those of the past. Information sharing is no more monolithic than any other complex issue or business process. Although information sharing is a good headline, when considering information sharing successes and failures we have to

"look under the hood" to see what is really going on, lest we fix things that weren't the problem in the first place.

While the mechanisms are in place for better information sharing, the fact is that we missed opportunities to stop the Christmas day bomber from boarding Northwest Flight 253, as well as opportunities to intervene before the Fort Hood shootings. In my view each of these represents a different challenge.

With respect to the first, information regarding the bomber was shared and shared widely. In the simplest of terms, the issue was not that people didn't have the data, but instead that they had too much data—and policy issues existed about what steps should be taken based on that data. With respect to the second, relevant information was not sufficiently recognized as such and passed to other operators, and FBI information technology hampered the connection of key data.

An enormous amount of intelligence information constantly pours into our National security system. Sifting through it, synthesizing it, making sense of it, and making sure it receives the necessary attention is a backbreaking challenge, one that requires attentive management and testing to determine where the flaws are and how to fix them. It also requires the latest software and technology to ensure that searches dive into all databases so that no pertinent information on an inquiry fails to be captured. That technology exists and is available today it simply needs to be widely deployed.

Of course, we should not view information sharing as an unmitigated good—or at least not as a good that does not require attendant modifications to other aspects of intelligence and homeland security as it advances. There is no greater illustration of this than the tragedy of WikiLeaks, which has disclosed to the world—both our adversaries and friends—sensitive information about our intelligence and policies. This publication of sensitive Government documents has harmed our Government's ability to conduct its affairs and has had serious consequences for our National security.

In my view WikiLeaks demonstrates why as we share information we must also increase our ability to control the information that is shared and take special care to control the wholesale movement of sensitive information off of protected networks. It is not new that those who wish to harm the Nation will attempt to steal our secrets; it is new that with the spread of electronic information they can steal petabytes rather than mere pages of documents.

STILL A NEED FOR IMPROVEMENT

Where, then, can improvements still be made? We offer some suggestions along the traditional lines of correction: Legal, policy, budgetary, personnel, and technology.

With respect to the first, legal, we must recognize that the Constitution and countless statutes govern the mosaic that is information sharing. In my experiences at NCTC, statutes ranging from the Foreign Intelligence Surveillance Act (FISA) to the Violence Against Women's Act drove what could and could not be shared. If there was one statute that was most at issue, however, it was FISA. In my view although FISA obviously provides critical protection of U.S. persons' privacy, it also makes for an exceedingly complex decision-making process within the intelligence community. Any way in which we can simplify this statute while maintaining protections would be invaluable for both collectors and analysts.

On the policy front, I believe it is important that we accelerate the review and adoption of Executive branch implementation guidelines for any information sharing-related policies. In my view the Executive branch has done an admirable job getting to the right polices in cases like the Attorney General Guidelines for various elements like NCTC, but the time required to adopt such policies borders on the Biblical. Yes there are difficult issues that must be addressed, but these issues are too important to allow the process to drag on as it most usually does.

Also on the policy front—but directly related to the budgetary—we remain concerned that FBI and DHS information-sharing efforts with State and local governments lack full cohesion. With declining budgetary resources, it strikes us as important to determine the best way to spend the marginal on DHS-sponsored fusion centers—where today the FBI has more people in place than does DHS. The U.S. Government must, 11 years after 9/11, ensure that respective Departmental foci are consistent with the reality of long-standing intergovernmental relationships and on-the-ground presence. I believe that the FBI's new responsibility as domestic DNI representatives is a very positive step in that direction.

Nowhere will budget play a bigger role in information sharing than State and local fusion centers, which are facing wide and deep budgetary challenges. In addition, budgetary issues will be faced in the context of protecting information from

leaks (which is required to enable information sharing), training for personnel on advanced analytic tools that enable information sharing, and having sufficient personnel to collect and exploit information so it can be shared effectively.

On the personnel front, many agencies must continue to train personnel to ensure that they know what information is relevant and hence what must be shared. In particular, the FBI needs to—as it generally has in the past—prioritize enhancing the status of its analysts and ensuring that analysis drives operations. Similarly, DHS must continue to improve its analytic cadre and move away from contract personnel. All analysts and operators must continue to receive high-quality training on issues like radicalization, to recognize signs of danger.

Finally, on the technology front, we continue to face a relative maze of Government information systems of significantly varying capability. We cannot be so naive to say that one big database of information can be created: This is neither technically feasible nor wise as it relates to protection of information and privacy. That being said, we must ensure that operators and analysts have advanced technology that allow them to make connections in disparate data sets, share their knowledge across organizations, and keep information secure. And perhaps most importantly, the Congress must continue to closely monitor Government information technology reforms as the bipartisan Executive branch record on this front is less than inspiring.

CONCLUSION

In sum, up until now the Government's counterterrorism capability has grown with much energy and devotion, but it has done so while flush with resources. The Nation's current fiscal situation means we have to be smarter in how we use our resources so that we get the maximum bang for our counterterrorism buck and can stay one step ahead of the ever-changing terrorist threat.

Our terrorist adversaries and the tactics and techniques they employ are evolving rapidly. We will see new attempts, and likely successful attacks. One of our major deficiencies before the 9/11 attacks was that our National security agencies were not changing at the accelerated rate required by a new and different kind of enemy. We must not make that mistake again. Sharing information rapidly is a major comparative advantage we have over terrorists. We must regularly review how we are doing and move quickly to address any problems, fill any gaps that arise.

Thank you for inviting me to testify, and for this subcommittee's leadership on these critical issues.

Mr. MCCAUL. I appreciate those comments, Mr. Leiter. Thank you for being here again; and I look forward to hearing the answers to my questions in a more open format, without the constraints of the Federal Government on top of you.

So with that, I would like to enter into the record a statement from the Honorable William Webster, the chair of the Webster Commission.

Hearing no objection, so ordered.

[The statement of Mr. Webster follows:]

STATEMENT OF WILLIAM H. WEBSTER, CHAIR, THE WILLIAM H. WEBSTER COMMISSION

SEPTEMBER 14, 2012

On December 17, 2009, Federal Bureau of Investigation Director Robert S. Mueller III asked me to conduct an independent investigation of the Federal Bureau of Investigation's handling of counterterrorism intelligence before and after the tragic shootings at Fort Hood, Texas, on November 5, 2009. The FBI had conducted an internal investigation in the immediate aftermath of the shootings and had implemented procedural, operational, and technological improvements. Director Mueller believed, however, that an objective, independent review was critical to understanding the FBI's actions and assessing the potential for further improvements.

I agreed to what proved to be a complex and lengthy assignment. The Terms of Reference were extraordinary in scope. Director Mueller requested not only a full investigation of the manner in which the FBI and its Joint Terrorism Task Forces handled and acted on counterterrorism intelligence before and after the shootings, but also a review and assessment of the FBI's governing authorities and the FBI's remedial measures in the aftermath of Fort Hood—with a particular focus on

whether existing laws and policies strike an appropriate balance between protecting individual privacy rights and civil liberties and detecting and deterring threats. That broad mandate was complicated, and its importance underscored, by subsequent terror-related events. The investigation did not probe the shootings, which are the subject of a U.S. Army-led inquiry and military criminal proceeding against Major Nidal Hasan.

In discharging my duties, I asked five distinguished citizens—seasoned investigators and legal specialists—to volunteer their time to serve as Commissioners: William M. Baker, Russell J. Bruemmer, Adrian L Steel, Jr., Kenneth L. Wainstein, and Douglas E. Winter. They were assisted by Stephen J. Cox, George Murphy, and Margaret-Rose Sales. Their contributions of time and energy were substantial, adding to the already significant demands of their work in the private sector. Their commitment to this investigation and the resulting report was an act of selfless patriotism.

The Commission took its responsibilities seriously. My colleagues and I pursued the sensitive, complex matters under review with diligence and care. The investigation was meticulous. Our discussions were vigorous. The Commissioners asked questions and expressed their perspectives, concerns, and opinions with candor. Although we disagreed from time to time during the course of our investigation, we were unanimous in our factual findings, our analysis of the FBI's actions, our recommendations, and every other aspect of the *Final Report.*

When I agreed to undertake this project, Director Mueller promised the FBI's full cooperation and support. That promise was fulfilled. The FBI and Department of Justice provided the Commission with more than 100 formal and informal interviews, meetings, and briefings; more than 10,000 pages of documents; and direct access to FBI computer systems. To obtain a broad range of perspectives, the Commission also consulted with outside experts on counterterrorism and intelligence operations, information technology, and Islamic radicalism; public interest groups that promote civil liberties and privacy interests; and staff from Congressional committees with FBI oversight responsibilities. The input of more than 300 persons and hundreds of documents informs the *Final Report.*

On July 12, 2012, after a completing the 2½-year investigation, we delivered the *Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009,* to Director Mueller. As you have seen, the Final Report exceeds 150 single-spaced pages in length and includes 18 formal recommendations for corrective and enhancing measures.

Director Mueller asked me to examine, among other things, "whether the actions taken by the FBI were reasonable under the circumstances known at the time." Our analysis of those actions could not proceed from what we later learned about Nidal Malik Hasan or Anwar Nasser al-Awlaki. Hindsight has uses, but it is not an appropriate tool for assessing the reasonableness and adequacy of actions taken without its benefit. Our review was based on information known or available to the FBI at the time the actions were taken.

We also recognized that reasonableness must be measured in the context of the FBI's governing authorities and policies, operational capabilities, and the technological environment of the time. For example, as discussed in the *Final Report,* the FBI's governing authorities limit its ability to disseminate information acquired using the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§1801 et seq., and require Agents and Task Force Officers to use the "least intrusive means" in conducting assessments and investigations. As a further example, the FBI's then-existing information technology and document review workflow did not assure that potentially relevant intelligence would be identified, correlated, and assessed in a strategic context.

Finally, we recognized our limited ability to predict what might have happened if different policies or procedures were in effect or personnel had made different decisions or taken different actions. We chose not to speculate. We examined instead the reasonableness of what did happen, in order to identify and recommend, when appropriate, better and corrective policies and practices for the future.

The *Final Report* did not hesitate to identify shortcomings when we found them. In its words: "We conclude that, working in the context of the FBI's governing authorities and policies, operational capabilities, and the technological environment of the time, FBI and Joint Terrorism Task Force personnel who handled relevant counterterrorism intelligence information made mistakes. We do not find, and do not suggest, that these mistakes resulted from intentional misconduct or the disregard of duties. Indeed, we find that each Special Agent, Intelligence Analyst, and Task Force Officer who handled the [intelligence] information acted with good intent. We do not find, and do not believe, that anyone is solely responsible for mis-

takes in handling the information. We do not believe it would be fair to hold these dedicated personnel, who work in a context of constant threats and limited resources, responsible for the tragedy at Fort Hood."

We concluded instead that "these individuals need better policy guidance to know what is expected of them in performing their duties, and better technology, review protocols, and training to navigate the ever-expanding flow of intelligence information." We also concluded that the FBI should continue to focus on compliance monitoring and the oversight of authorized investigative techniques that may affect privacy rights and civil liberties.

The Commission found shortcomings in FBI policy guidance, technology, information review protocols, and training. We made 18 important recommendations for corrective and enhancing measures in those areas and about the FBI's governing authorities. We also identified, but took no position on, two legislative actions that the FBI could propose to improve its ability to deter and detect terrorist threats. Finally, we assessed whether administrative action should be taken against any employee involved in this matter, and we concluded that administrative action was not appropriate.

The FBI has agreed with the principles underlying all 18 of our recommendations. In most cases, the FBI has taken action to implement the recommendations based a combination of the Commission's work, its own internal review of the Fort Hood shootings, and the report of the U.S. Senate Committee on Homeland Security and Governmental Affairs.

I appreciate the subcommittee's interest in the lessons of Fort Hood. Those lessons are not specific to the Federal Bureau of Investigation, but resonate throughout the law enforcement and intelligence communities. The *Final Report* provides insights into the arduous mission of the FBI and other agencies in combating the threat of terrorism, whether domestic or international.

Throughout our investigation, we witnessed the ever-increasing challenge that electronic communications pose to the FBI's efforts to identify and avert potentially destructive activity. Although our Report reviews the specifics of one tragic event, it also speaks to transcendent issues that are crucial to our ability to combat terrorism in the electronic age.

We did recommend corrective and enhancing measures, but nothing said in the Final Report is intended to cast doubt on the dedication and professionalism of the men and women who serve our Nation in combating terror and crime.

Thank you.

Mr. MCCAUL. I want to just show, not for any reason other than—this was taken the day of the memorial service at Fort Hood, and you can see—I was standing here—you can see the boots, the rifles, the helmets. It really gives you a graphic picture of what really happened that day.

[The information follows:]

Mr. MCCAUL. You can see one of these soldiers on crutches. I asked him, "What did he say when he shot you?" "Congressman, he said 'Allahu Akbar,'" God is great, the classic jihadist terminology.

At that moment, I realized that this was not a workplace violence incident, that this was something more, that this was in fact an act of terrorism. I was criticized at the time for saying that. I think history will judge that as a correct assessment of what happened on that fateful day.

Mr. Leiter, I want to start with you, because you headed the NCTC. You are really the expert at connecting the dots, and you did perform a masterful job while you were there.

You and I worked with Joint Terrorism Task Forces. They have an enormous challenge, an enormous amount of data that comes through, and many of which, if you miss one thread of evidence, you can be held accountable by Members of Congress like myself at a later hearing.

But these emails, the 18 emails that took place, when we were briefed by senior intelligence officials—and they wouldn't give us the content, they would just simply say—the only word I can use is downplay the significance of these emails. Finally, when the good work of the Webster report revealed these emails publicly, we all had a chance to actually read the content.

The one that I described in my opening statement on May 31, 2009, Major Hasan, he almost seems to be telegraphing exactly what he is getting ready to do, almost asking for permission from al-Awlaki in Yemen, is it okay for a suicide bomber to kill soldiers and innocent civilians in the cause to protect our fellow brothers?

You know, you and I have worked in law enforcement. This is one of 18. The other one, "keep me on your Rolodex," you know, to me, this is a huge flag.

It was a big deal in San Diego. The San Diego Joint Terrorism Task Force thought, wow, there is something wrong going on here. We need to start—let's send a lead to WFO. Let's have them investigate.

The response from WFO is astounding, that, well, we don't really see a terrorist threat here; and they basically shut down this investigation until 5 months later when Major Hasan kills 13 people, 12 soldiers.

There is a Department of Defense official on the Joint Terrorism Task Force, and yet that official didn't contact Fort Hood. Maybe it is the legal restrictions that you are talking about. If so, we need to change that.

There were so many flags not only between the FBI two offices—and I really commend the San Diego office for their courage and bravery of trying to get to the bottom of this. I fault the WFO office for not following up on this. In the military, the way they passed this guy along, knowing he is proselytizing radical Islam with a business card: Soldier of Allah. He is enraging his colleagues. What do they do? They don't want to deal with the problem. They want to pass him along, promote him, send him down to Fort Hood.

So many flags in this case. The dots were identified, but they weren't shared. How did this happen?

Mr. LEITER. Congressman, I will say that I agree with you that it did not take long, from my perspective, to know that this was an act of terrorism. In fact, the National Counterterrorism Center within a week of the event entered this into its world-wide database of terrorist events based on preliminary reports. That was not a conclusive legal judgment but certainly all the indications were that this was terrorism.

I think in terms of the information that was not shared, you had a breakdown along so many different angles. The San Diego team I think did do a very good job; and I would defer to Mr. Winter, of course, who knows these details better than I, but they were not even aware of all of the emails. They were not aware of the Department of Defense information. WFO was not aware of much of that. It was handed to an officer who, frankly, from an outsider's perspective, I think didn't have a really strong understanding of the signs of radicalization.

Now, the two points I would make quickly in defense of how this evolved is: No. 1, we do have to put ourselves back in 2009 to recall who Anwar al-Awlaki was then versus who he is perceived to be today. In 2011, 2012, we understood him to be an operational leader in a way that in 2009 we did not. That is not an excuse, but it is some color.

The second piece is, from my perspective, Congressman, the idea that people would not go talk to him I do not understand. I do believe that if that information were shared with a broader group who understood radicalization there would have been increased pressure from headquarters to make that happen; and that would have led to, I believe, a better outcome.

Mr. MCCAUL. I couldn't agree with you more.

I talked to the commanding officer at Fort Hood. Wouldn't you have liked to have known this? I understand FISA complications. I understand you want to shake down somebody. They could have at least watched him, put him under some sort of surveillance. Just maybe that would have stopped what happened.

My time is limited. I do want to go to Mr. Winter.

Eighteen emails, WFO only has two emails. Some technology breakdown occurs where they are not even aware—they can't even access, they didn't even know how to access to get these remaining emails. I have to say, Mr. Leiter, I mean, you as a former Justice Department official like myself, this May 31 email, if you read this, would that concern you?

Mr. LEITER. Congressman, I look at one email and I look at the body of the emails and to me they are clear indicators of an individual who has been radicalized. Whether or not he has been mobilized to take action, that is a hard call——

Mr. MCCAUL. But when he is asking permission to perform a suicide bombing mission against soldiers and civilians at a dinner to protect his fellow——

Mr. LEITER. That is why I said, Congressman, I would want somebody to go out and interview this guy, who has clearly been radicalized.

Mr. MCCAUL. I think that is what should have happened in this case.

Mr. Winter, what happened here?

Mr. WINTER. The decisions made in WFO were based on a cascading set of circumstances.

Mr. MCCAUL. Your microphone?

Mr. WINTER. I am sorry. Is that better?

Mr. MCCAUL. Yes.

Mr. WINTER. The decisions made at WFO were the result of truly a cascading set of circumstances. San Diego sent this lead based on the first two emails that were acquired from Hasan to al-Awlaki. There was no FBI policy on the assignment of these types of leads or on taking action on these types of leads.

The supervisor of WFO waited 50 days after the arrival of the lead to read it and to assign it. He assigned it to a DCIS agent who was a task force officer.

That agent waited 90 days from then to read it and to act on it. Under informal FBI practice, agents had 90 days to work on leads, either to elevate them into an investigation or to close them down. So this agent read that lead and acted on it on the last day under that FBI practice and, indeed, conducted this assessment in 4 hours on that day.

So it was rushed. There was that pressure that was created by their workload and these late assignments.

He consulted U.S. Army electronic personnel files on Major Hasan. That was the entirety of what he as a DCIS agent could have access to from the JTTF. That meant he received a brief and highly misleading set of personnel records that indicated that Major Hasan had a security clearance, he had been promoted to major only 10 days earlier, and his supervisors praised him thoroughly. The only negative in those 80-some pages, I believe, was that he had failed his PT test.

Mr. MCCAUL. They praised him.

Mr. WINTER. They praised his research on Islam in the military.

Now, Hasan had used his real name in communicating with al-Awlaki, so had not tried to render himself anonymous. The DCIS agent concluded, based on that, that this was part of Hasan's research on Islam in the military and that the Army approved of it.

At the same time, there was no FBI policy on what is called a baseline collection plan. That policy was instituted in September, 2009, after this investigation but before the Fort Hood shootings. That created a minimum of what agents are meant to collect when conducting an assessment. If that plan had been in effect then, this agent would have been required to consult the DWS–EDMS system, which is a computer database on which all of the messages from Hasan to al-Awlaki and vice versa were stored. Thus, he would have known of that, and he would have been required to search it.

But he had not been trained on that database. He didn't even know it existed. So, what he believed, after searching FBI databases, was that there were only two emails, that they were sent in December, 2008 and January, 2009, which was 5 months prior, and that al-Awlaki had not responded. Based on that, he concluded and his supervisor concluded that Hasan was not involved in, "terrorist activities."

Now, did that resolve the question of whether or not Hasan was a threat? We didn't believe so. We felt that this decision-making

process was flawed and that they should have considered and conducted an interview of Hasan based solely on the information they had at that time.

But I am not defending the decision; I am explaining it. You can understand how reasonably these men could have been led down this path by the combination of all these circumstances, some of which were self-imposed, others of which were the result of the lack of policy, others that were the result of an inability to gain access to those records that Walter Reed, for example, had.

Mr. MCCAUL. I think those problems need to be fixed. But I will ask you this question. I believe that gross errors were made in this matter that resulted in 13 people being killed, 12 soldiers. Should anybody be held accountable within the Federal Government?

Mr. WINTER. On our review—we were specifically asked by Director Mueller to assess whether any disciplinary action should be taken against any of the personnel involved. Although we found that mistakes were made, we found that these individuals acted with good intent, they acted mostly reasonably under the circumstances, and that they were not individually responsible for some of the decisions that occurred because of the lack of policy direction, for example.

One of the reasons we advocated the seven policies that we recommended was that if those policies had been in place, and similar procedures, then actions like this would violate them and individuals would be directly responsible and subject to discipline.

Mr. MCCAUL. Is it your understanding these policies are in place now?

Mr. WINTER. Almost all of the policies are in place. They are not—some of them are being coordinated into a single policy, the command-and-control hierarchy, for example.

Mr. MCCAUL. My time is kind of running short.

On the Center report, they indicated the San Diego office calls WFO; and the response back is: Look, we don't want to damage his stellar career, and something to the effect of this is a politically sensitive matter.

That was not corroborated by the WFO office. Is that correct?

Mr. WINTER. That is correct.

Mr. MCCAUL. But, according to San Diego, that conversation took place.

Mr. WINTER. Well, the first part that you discussed is corroborated, that WFO advised San Diego twice that they did not believe an interview of Hasan was appropriate because it would damage him in terms of his position in the military. The chain of command would not take it lightly.

Mr. MCCAUL. I do think that the American people and the families and the victims deserve that somebody in this Government be held accountable for what happened.

Professor, I want to ask you real briefly, with my limited time left, you spoke very eloquently of your experience of the fear of speaking out. Within the Department of Defense, you know, we have this individual that various of his colleagues are seeing these warning signs popping up. They call him a ticking time bomb. He is proselytizing radical Islam, talking about Osama bin Laden, having business cards that say Soldier of Allah. I mean, so many indi-

cators are there, and then no one wants to speak out. There is a fear of retribution within the Army, and he is just sort of passed along. Is this a case where political correctness was more important or overshadowed National security?

Ms. MANJI. It sure sounds like that—if you can hear me, it sure sounds like that.

Thank you.

It sure sounds like that, Congressman. Frankly, I think it would be fairer to ask if political correctness also crept into the FBI.

For example, we have spent the last several minutes talking about how somebody at the San Diego office of the FBI had a troubling lead, passed it on to the Washington field office, after which it went nowhere. One of the questions I have, as I am listening to these other testimonies, is why did the San Diego officer not stand up when it became clear to him or her that an obviously unsettling lead was not going to be acted upon?

Now, one can argue that, well, it is obvious why people don't stand up in general, because doing so invites complication in your life. Life is complicated enough, thank you very much.

But this is where I believe we can actually learn something about a mechanism that the Department of State has put into place, and that is a mechanism called the dissent channel. It was actually introduced just after the Vietnam war, whereby foreign policy officers, when they see that the chain of command is going to be resisting their dissent with groupthink, with the settled consensus that has been accepted for too long within the cozy confines of that department, they can actually use this dissent channel to explain why somebody higher up needs to hear a counter argument. They do not have to get permission from their higher-ups in order to be heard through this channel.

I don't think that that exists either at the Department of Defense or at the FBI, but it is something well worth investigating whether it works, as it did, by the way, in the lead-up to the Yugoslav—to the Balkan genocide. It was, one could argue that that was the reason, because at the time Secretary of State Eagleburger heard a dissenting voice through that channel and realized that the United States must intervene.

It was through that that I think we can learn a little bit more about how dissent can be institutionalized so that it is constructive rather than chaotic.

Mr. MCCAUL. Thank you. Excellent point.

The Chairman now recognizes the Ranking Member.

Mr. KEATING. Thank you, Mr. Chairman, and I think you have done a good job of looking historically at this.

I want to come at this at a different angle, maybe ask Mr. Leiter first. I have heard about the policies. I have heard about some of the changes. Could this, under the same set of circumstances, happen today?

Mr. LEITER. Congressman, you would end up with a slightly different set of facts. It wouldn't quite fit the policies that you put in place, but I think that there remain holes.

Mr. KEATING. Forget the policy, just the circumstances.

Mr. LEITER. I think it is less—the more it looks like this circumstance, the less likely it is going to occur. But could something like this fall through the cracks? Absolutely.

I still believe that there is information that is not being shared effectively and, quite often, that information is about U.S. persons, which is appropriately the most protected set of information; and the Congress and the Executive branch must ensure that that information is effectively shared. So, as the professor very ably said, you can get second and third opinions and you aren't simply forced to take the views of one operator or one analyst about whether or not someone is a threat.

Mr. KEATING. Mr. Winter, could this still happen today?

Mr. WINTER. Absolutely. I agree with Mr. Leiter, the closer the circumstances to those of the Hasan matter the less likely it is to happen because of the policy changes, because of the higher sensitivity to these types of issues.

For example, however, two of our recommendations concern the FBI putting into place a clearinghouse process by which—which it currently has with DOD—by which it advises DOD through headquarters and through the National Joint Terrorism Task Force about investigations of DOD personnel in the military. We recommended that similar clearinghouse procedures be adopted for law enforcement agencies, whose Members may have equal if not greater access to weapons and intelligence than military members and also as to other departments of the Federal Government.

So that if someone at the State Department is under investigation there is a mechanism in place for the investigating officers to move that not only up the FBI chain of command but also move it to the State Department chain of command and their investigators so that all the individuals can work together to detect and deter the potential for terrorism.

However, obviously, outside of Government hierarchies, the possibilities for individuals like Major Hasan to take these kinds of actions exist; and it is difficult for the FBI to have constant knowledge of the whereabouts and intent of those types of individuals.

Mr. KEATING. One thing that—I wasn't going to ask this, but you sparked this interest. I have asked it of General Barry McCaffrey before. That initial information, getting to whether it is local or State officials usually, how is that inhibited by not having a comprehensive immigration policy in the State? If people see things, if people want to come forward, how are they going to come forward if they are going to effectively make themselves criminals? How weak is that in the initial information?

Mr. WINTER. That is something that is slightly beyond my pay grade, sir. I would try to answer in this fashion, however.

The FBI has in place what is known as an eGuardian system, which is an electronic version of its Guardian system, by which individuals who bring information to local law enforcement agencies, let's say, even anonymously, tips and the like, can be forwarded on immediately and promptly by electronic means and acted on by FBI agent reviewers and analysts, I should say, within a very short period of time.

Mr. LEITER. Congressman?

Mr. KEATING. Assuming they did that.

Yes, Mr. Leiter.

Mr. LEITER. I think interaction with immigrant communities is critical. In the counterterrorism context, obviously what we are most focused on is American Muslim communities, which may or may not be immigrant communities. But engagement by the FBI, the Department of Homeland Security, Immigration, a wide range of agencies and State and local officials with American Muslim communities is absolutely critical to occur not just for law enforcement intelligence but for good Government and engagement.

I will say that Congress has an important role in that regard, that when the FBI does engage these Muslim communities that they are not immediately second-guessed about which Muslims they talk to. It is very important for them to have wide engagement to understand these communities and potentially identify individuals who have been radicalized. In my view, the Congress has to give the Executive branch reasonable room to maneuver to do that engagement to find problem areas.

Ms. MANJI. May I add something of my own in this regard?

Mr. KEATING. Just briefly, yes.

Ms. MANJI. Sure.

Of course, engagement with communities of all kinds is necessary for good governance. The problem is that, too often, especially in this country, we stumble over ourselves to try to identify who are the moderates and who are the extremists. I would argue to you gentlemen that this is the wrong distinction.

The better distinction to make, if you want to really get at the heart of the matter, is who are the moderates and who are the reformists. Moderates, for example, don't much differ from extremists in that moderates are so consumed with what they perceive to be Western imperialism, Israel, America, so forth, that they have distracted themselves from dealing with the imperialism within their communities, those clerics, those imams, and even those supposedly secular civil leaders who insist that good Muslims remain silent when crimes such as honor killings happen within their communities.

So we need to ensure that we get the framing here right if you are actually going to hear people who are willing to step forward. But they are not going to be willing to step forward, Congressman, unless they know that you have got their back. Because they know what backlash is coming their way by virtue of having opened their mouths.

Mr. KEATING. Thank you. Thank you.

I just want to get back to the process itself, too.

One of the things that you said, Mr. Leiter, that concerned me, is—because we hear it all the time in this committee in particular in different shapes and forms—but you used the word the necessity of having a National system versus a patchwork system. To me, we could have the greatest information in the world coming forth. If we don't have a way to process that on a National basis—can you really talk more specifically about what you meant when you said that? I mean, how far along——

You know, all of DHS is patchwork, as far as I am concerned. It is amazing that we haven't gone past jurisdictional issues and

done some of these things yet. But, to me, that has to get fixed first.

Now, I know we have budgetary issues in front of us. But if that is not fixed and that is not a priority, what good does all this gathering of information, what good is it?

So when you said that, you know, I think that is a priority that we have to have. What budgetary issues are confronting that and what actual technology issues or interaction issues with different levels of intelligence? Expound on that.

Mr. LEITER. Congressman, absolutely. We obviously, as both you and the Chairman know well as attorneys, we live in a very Federated system. As we built up these State and local fusion centers with hundreds of millions of dollars, that information is being collected at the local level and, to some extent, shared with Department of Homeland Security and the FBI through the JTTFs. But what we have not done is created a system where you can actually effectively compare that information across State and local fusion centers, across JTTFs.

Now, I think the FBI took a very, very valuable step in the past year, which is to move toward a regionalized structure. Because I don't believe that you can have any system with 104 JTTFs and 50-plus fusion centers and actually see correlations quite effectively. So a regionalized intelligence structure, where you have I believe it is six or eight regions that are looking at the various State and local fusion centers and JTTFs and seeing where there is suspicious activity or where there is a FISA intercept of import. Then having those cases managed by the FBI headquarters, in coordination with DHS, that starts to look like a system.

As you see that and as that information is shared within the Federal family, with the National Counterterrorism Center, with Homeland Security, who is specializing on borders, using their collection resources, and ICE and Customs and Border Protection, you start to understand how you can close these gaps and, as you so eloquently stated at the beginning of your questions, try to avoid this from happening in the future.

As budgets go down, weaving this together will be more difficult. But absolutely the technology exists today to make sure that some of those less understandable correlations are seen both at the State level, at the local level, and ultimately at the Federal level for some of these cases.

Mr. KEATING. Just a last quick question of yourself and Mr. Winter. Would you say that is among the top priorities right there in having that occur?

Mr. LEITER. Yes.

Mr. WINTER. I absolutely agree. That was the first of our information technology recommendations to the FBI, enterprise data management.

Mr. KEATING. Thank you very much. I yield back.

Mr. MCCAUL. Thank the Ranking Member.

The gentleman from South Carolina, Mr. Duncan, is recognized.

Mr. DUNCAN. Thank you, Mr. Chairman. Thanks for this very timely hearing.

You know, the State Department had warnings at least 48 hours in advance of the 9/11 attacks that happened this week, yet they

did not go in lockdown in certain embassies where the threats were. The reason I say that is a lot of times we are given very, very clear signals, staring us in the face, and we fail to act on those.

Or many times we lean back on political correctness. As Professor Manji pointed out, the religious symbolism, the Operation Badr, they didn't even want to discuss the real ideology behind a certain terrorist attack, the fact that we have here in America taken to calling the Fort Hood a case of workplace violence, yet we will call what happens in Wisconsin an act of domestic terrorism.

I am alarmed and really want to raise awareness here in this committee of some of the things that I hear going on within our Pentagon and within the military, where servicemen and women are discouraged from pointing out things that they see such as what happened at Fort Hood with SOA on the card, and just signals that are very clear for people that are going through their daily routine that should raise a red flag for us. But yet they are scared they are going to be labeled as an Islamophobe.

I think when we have hearings within this committee addressing Fort Hood or addressing the radicalization of Muslim youth, it is not an address of Islam, it is more of an address of an ideology that is really encouraging folks that practice Islam as a religion to embrace a certain set of ideals and ideological values that lean more toward the attacks that we see. I think that is what happened. Major Hasan was caught up in that.

But, as Americans, we can't be afraid to speak out. I want to thank the professor for having the courage, the moral courage to speak about those differences—that is what I heard today—about the difference between Islam and your practice of the Islamic religion, but also the fact that, you know, there are some folks that do practice that religion who have gone in another direction in another part of their life in their political ideology and what their world vision is.

So one thing I want to ask all of you is, following the findings and recommendations of the Webster report on the Fort Hood attacks, how would you categorize the attack that occurred at Fort Hood? Mr. Winter.

Mr. WINTER. We discussed this question at length. I speak for the Commission and our unanimous view. Our view was that we saw evidence but we did not have the opportunity to investigate on a criminal basis, as the U.S. military is doing, and so we don't know——

Mr. DUNCAN. Let me ask this question a different way. Workplace violence or domestic terrorism?

Mr. WINTER. I have heard that, both of those characterizations. We refused to reach a finding on that. I have to say the reason is that we don't have the evidence sufficient to know. We don't know what kind of standard Department of Defense is applying.

Certainly our investigation was not into Department of Defense activities; and it was not into the criminal investigation itself, which was to a great degree hands-off to us because the military is pursuing that criminal case against Major Hasan. So we were unable to reach a decision on those issues. We do believe and really would like to see justice done for the victims, their families.

Mr. DUNCAN. I am going to end this dance.

Professor Manji.

Ms. MANJI. Domestic terrorism, home-grown.

Mr. DUNCAN. Thank you.

Mr. Leiter.

Mr. LEITER. Congressman, the analysts at NCTC within a week, as I said, deemed it to qualify as an act of international terrorism under our statute that we use. It was a subgovernmental group, political violence. We called it terrorism then; I call it terrorism today.

Mr. DUNCAN. Okay. I want to refer back to the Chairman's opening statement. The men and women that stood at Fort Hood at that ceremony, ones that were wounded in that attack, the families of the victims of that attack will tell you to this day this was an act of domestic terrorism in the war against terrorism. I think we as America need to set aside political correctness and really be able to discuss the real threats, existential threats to our way of life.

With that, Mr. Chairman, I yield back.

Mr. MCCAUL. Thank the gentleman.

The gentleman from Illinois, Mr. Davis, is recognized.

Mr. DAVIS. Thank you very much, Mr. Chairman; and I certainly want to thank the witnesses for their participation and especially for their insights and their answers.

I was thinking that, you know, we can always know what happened because we have the information. It is obviously far more difficult to determine why it happened or the causes that may have generated or caused it to take place.

Mr. Winter, let me ask you, if I could, you indicated that policies are that investigators and agents have 90 days to work on leads and that sometimes individuals have more call for activity than time or there is not enough personnel, there are so many leads and trying to follow up on all of them. Are there thresholds that will jump out at you? I mean, if you are reviewing tips and information and allegations, that a person can just kind of see that this appears to be over the line and we need to try and check it out as quickly as we can?

Mr. WINTER. Yes, there is a significant amount of training on many different levels on how to deal with tips, information, intelligence of different kinds. Here the San Diego agents recognized that the messages deserved some form of action. Under FBI policies that then existed, they could set what was called a routine discretionary action lead because it was not—there was no indication of anything imminent, something that required a 24-hour or 48-hour response. That meant it was a routine lead, which would be resolved in the ordinary course of business. It also meant that the WFO would exercise its discretion on how to handle the lead.

The 90-day period that was in existence was an informal FBI practice at that time. We have, of course, recommended that the FBI establish periods within which leads must be acted upon. The FBI in turn has also eliminated these discretionary action leads and has required action on all leads that are sent out from other offices.

Mr. DAVIS. Let me ask each one of you if you think that we do as well as we possibly could in making assessments of individuals when they are going to be placed in certain kinds of positions rel-

ative to evaluation as people seek employment, as people take assignments and have access to certain kinds of opportunities. Do we assess their personalities or do we glean enough information where it gives a comfort level in terms of where they are and what they might be doing?

Mr. LEITER. Congressman, I will answer on two pieces.

First, I think we probably all as bosses have interviewed someone, given them a job. They had glowing recommendations, and then they come and work for you and the performance ain't so glowing. So this is a pretty broad problem. Obviously, the manifestation in this situation is absolutely tragic.

The second piece, though, more specific to terrorism, is the FBI does have an incredibly difficult job of distinguishing those people who were radicalized and have radicalized views and those who become mobilized and actually take a terrorist action. Again, that is why you want people to go out and interview them and try to make that determination.

But, frankly, the FBI, with all its resources, if you used everyone in the Federal Government, they couldn't watch everyone who was just, "radicalized." They have got to prioritize. Making that determination is very hard before the fact and looks very, very easy after the tragedy.

Mr. DAVIS. Or even people who might seek to become members of the FBI to be in a position to carry out their ultimate aim.

So all I am really seeking is opinion. I know that it is tough trying to deal with motivation all of the time. I mean, if we could answer that, we would be in very good shape.

Ms. MANJI. Congressman, if you will allow me one quick intervention, I have written exactly about this question of what to ask in order to conclude within the Muslim communities of this country where people stand on the continuum of reform, moderation, extremism; and I would be very pleased to submit to the committee the specific questions that I recommend be asked.

Mr. DAVIS. Thank you very much.

Thank you, Mr. Chairman.

Mr. MCCAUL. I thank the gentleman.

Just let me close by—first, let me thank you for this excellent testimony. I agree with you, Mr. Leiter, that the FBI, JTTFs have an enormous challenge. So much information is coming through, and you miss one thread and then you are held accountable.

I think this case, though, I would make the argument is a little different. You have got a major on a base, Fort Hood, who is talking to a cleric, who there was some evidence may even have had ties to the 9/11 hijackers, for God's sake, and he is really rising in stature to becoming the No. 2 in the world, next to bin Laden.

I think, unfortunately, WFO only gets two emails. They don't get the May 31 email that clearly outlines what his intentions are and what he is planning to do.

You are right, Professor, San Diego has it, though; and they have DOD employees on these task forces. You know, why didn't one of those at least contact Fort Hood? Why didn't anybody contact Fort Hood and say, you know what, there is an issue here? You got a problem. You got a guy that could actually kill somebody, you know.

I don't think any of you really have the answer to that. I don't have the answer to that. It is just unfortunate that it didn't happen in this case.

So with that, again, we thank you for your brilliant insight and your excellent testimony; and I will dismiss this panel, move onto Panel No. 2. Thank you.

[Off the record for a few minutes.]

Mr. MCCAUL. Our Government witness requested to be on a separate panel all by himself.

Let me introduce Mr. Kshemendra Paul, who is the program manager for the Information Sharing Environment at the Office of the Director of National Intelligence. As program manager, Mr. Paul has Government-wide authority to plan, oversee the buildout, and manage use of Information Sharing Environment. He also co-chairs the White House's Information Sharing and Access Interagency Policy Committee.

The Chairman now recognizes Mr. Paul for his testimony.

STATEMENT OF KSHEMENDRA PAUL, PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. PAUL. Chairman McCaul, Ranking Member Keating, distinguished Members of the committee, thank you for inviting me to testify today.

My is Kshemendra Paul. I am the program manager for the Information Sharing Environment. By training and profession, I am an information technologist. Formerly, I was the chief architect of the Federal Government.

My office works with mission partners—Federal, State, local, Tribal, private sector, and internationally. Together, our focus is on the improvement of the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information.

The role of my office is planning, oversight, and management. We span a variety of communities—law enforcement, homeland security, defense, foreign affairs, and intelligence.

As my office and our partners continue to implement responsible information-sharing practices, we reflect on the progress we have made across the Nation, as well as recognizing that work remains.

In January, Director Clapper spoke of a National responsibility to share information. He encapsulated our vision. He said, and I quote, "The right data, anytime, anyplace, usable by any authorized recipient, preventable only by law and policy and not technology and protected by a comprehensive regime of accountability."

This week, we marked the 11th anniversary of the 9/11 terrorist attacks. The National security community has achieved numerous successes. As they pertain to my office, these include improving interoperability of our sensitive but unclassified networks, enhancing the capabilities of the fusion centers, State and local fusion centers, expanding the mission application and the impact of the Nation-wide Suspicious Activity Reporting Initiative, strengthening industry and Government adoption of our interoperability and standards framework, including the National information exchange model, and, finally, integrating our non-Federal stakeholders, in particular State and local law enforcement, into the National policy

conversation through the interagency policy committee you mentioned.

But we are not without challenges. These include the continuously evolving threat environment, the tsunami of data faced by my mission partners, and the constrained fiscal environment.

My office continues to convene partners and lead efforts in responsible information-sharing innovation. This is a journey. The evolution of the threats against us, the integration of our resources, and the efficient use of technology require constant vigilance and leadership. The threats to our safety do not stop at jurisdictional or agency boundaries. Our information shouldn't either.

Three core ideas are the drivers of the mission of my office. We are grounded by an enduring purpose to advance responsible information sharing to further the counterterrorism and homeland security missions. We are focused on responsible information sharing to enable decisions to prevent harm to the American people. Finally, we are building capacity for responsible information sharing across our mission partners at all levels of Government.

We are also strengthening protections for privacy, civil rights, and civil liberties. This work makes us stronger.

Let me elaborate. Every fusion center in our country has a privacy policy as comprehensive as Presidential privacy guidelines. The bulk of Federal departments are in the same position, and we are well on the way to finishing the job here in Washington. This means that when citizens see something and say something, when police officers submit reports to fusion centers and Joint Terrorism Task Forces, when analysts work to connect the dots, the work proceeds across agencies and levels of government in a standardized and efficient manner that handles information appropriately and responsibly.

Gaps, challenges, and opportunities for improvement exist. We have traction, a clear and compelling value proposition, and a way forward to continue to accelerate responsible information sharing. You have our comprehensive annual report; and, for the record, it is located on our website, ISE.gov.

In summary, I believe there is no higher priority in the nexus between National security and public safety than responsible information sharing.

On a personal note today, as we talk about the attacks at Fort Hood and also reflect on recent events overseas, I just want to say that my thoughts and prayers go out to the victims and their families.

Mr. Chairman, Ranking Member, thank you for the opportunity to be here, and I look forward to your questions.

[The prepared statement of Mr. Paul follows:]

PREPARED STATEMENT OF KSHEMENDRA PAUL

SEPTEMBER 14, 2012

INTRODUCTION

Chairman McCaul, Ranking Member Keating, and distinguished Members of the subcommittee, I am Kshemendra Paul, the program manager for the Information Sharing Environment (ISE). We are the National office for responsible information sharing. The ISE provides analysts, operators, and investigators with information needed to enhance National security. These analysts, operators and investigators

come from a variety of communities—law enforcement, homeland security, intelligence, defense, and foreign affairs—and may work for Federal, State, local, Tribal, or territorial governments, or in the private sector or our international partners. The PM–ISE works with ISE mission partners to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information. The primary focus is any mission process, anywhere in the United States, that is intended or is likely to have a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. The PM–ISE facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices.

STATEMENT

As PM–ISE and our mission partners continue to implement responsible information-sharing practices, we reflect on the tremendous progress made toward our goal, while recognizing that significant work still needs to be done. In January, Director of National Intelligence James R. Clapper spoke of the National responsibility to share information—"the right data, any time, any place, usable by any authorized recipient, preventable only by law or policy and not technology, and protected by a comprehensive regimen of accountability."[1] As the office responsible for organizing and implementing responsible information-sharing practices Nation-wide, we are proud of the progress we have made strengthening National security while also honoring and protecting privacy, civil rights, and civil liberties.

We have become much better at using our inherent strengths to make the American people safer. Our federated democracy means that we have committed law enforcement, public safety, and intelligence professionals working at the Federal, State, local, and Tribal levels; they are also working closely with partners in the private sector to protect our Nation's infrastructure. We have carved out a strong role for governance through our leadership role in the White House's Information Sharing and Access Interagency Policy Committee. Our robust and innovative private sector contributes significantly to the work of the ISE. And we are championing a standards-based approach to defining Government requirements for responsible information sharing that will enable greater interoperability across our Government's networks while offering a greater potential for cost savings.

This week we marked the eleventh anniversary of the 9/11 terrorist attacks. The National security community has achieved numerous successes since 2001, including progress towards improving: Interoperability of our sensitive but unclassified computer networks, capabilities of our fusion centers, and mission impact of our Nationwide suspicious activity reporting practices. The PMISE has enhanced our National security by: Advancing these initiatives, brokering solutions between organizations with different missions, convening partners from inside and outside the Government, and leading improvements in responsible information sharing through policy, governance, and strategy.

The PM–ISE is committed to continuing to convene partners and lead efforts in innovation. We understand that this is a continuing journey. The evolution of the threats against us, the integration of our resources, and the efficient use of technology to move our responsible information sharing agendas forward requires constant vigilance and leadership.

Three core ideas are the drivers of PM–ISE's mission. We are:

- Grounded by an enduring purpose to advance responsible information sharing to further the counterterrorism and homeland security missions. We must stay focused on the fact that we are sharing information in order to keep the American people safe.
- Leading a transformation from information ownership to information stewardship in order to improve Nation-wide decision making. We must treat information held by the Government as a National asset: This means it must be used, and reused, to benefit the American people. Information must be protected and cultivated to ensure that we get the maximum value from it. At the same time, strong protections for the privacy, civil rights, and civil liberties of the American people must be safeguarded.
- Promoting partnerships across Federal, State, local, and Tribal governments, and the private sector, as well as internationally. By building organizational capacity at every level, we will share information more securely and effectively. The threats to our safety do not stop at jurisdictional borders; our information must not either.

[1] *http://csis.org/files/attachments/120126__info__sharing__clapper__transcript.pdf.*

We have also strengthened privacy, civil rights, and civil liberties protections by developing privacy guidelines, on behalf of the President, and supporting Federal, State, and local agencies as they develop privacy policies that are at least as comprehensive as the ISE privacy guidelines.[2] This means that when citizens see something and say something, and when police officers submit reports to their local fusion centers, they all know that the information will be handled appropriately. It means that when analysts conduct their evaluations, they will proceed in a manner based on agreed-upon definitions of behaviors that are indicative of terrorist activity, and that their investigations will not be based on race or religion. It means that the American people can know that their Government is committed to protecting their privacy, civil rights, and civil liberties, as well as their security.

While we focus on the accomplishments and the progress to date on numerous fronts, we maintain a sense of urgency about tackling the work that remains to be done. The biggest challenges facing the ISE are the continuously evolving threat environment, the tsunami of new data, and a constrained fiscal environment. As the ISE grows and its work deepens and expands, we need to continue to assess and adjust for current realities—allowing us to be well-positioned for dealing with future threats and exploiting opportunities.

These challenges and opportunities present a framework within which to rethink the ISE and our approach to responsible information sharing. We see great potential in leveraging our advances and building from the terrorism-related mission to more broadly support information-led public sector transformation. Recognition of the enduring value of the ISE lies in the ceaseless needs of the mission and the variety of continued successes that have been spawned by our work. The 2012 ISE Annual Report to the Congress showcases many of these accomplishments and lays out our way forward. While gaps, challenges, and opportunities for improvement are present and described, we have established traction, developed a clear and compelling value proposition, and identified a way forward.

We are fulfilling the mission set out before us, and we are enhancing our National security through responsible information sharing. We will continue to fulfill this mission and to identify and meet new challenges as they arise.

More information about the Information Sharing Environment and the office of the Program Manager is available at ISE.gov.

SUMMARY

I believe there is no higher priority for our National security than the issue of information sharing. Congress has provided us the mandate through legislation; the President has provided us the leadership and further guidelines; we continue the work of transforming our information-sharing environment into one that works more effectively for all.

Thousands of men and women work tirelessly to protect this Nation from terrorist threats. It is important for us to provide them and other decision makers with the best possible information to do their job to protect the people and interests of the United States against another terrorist attack.

Mr. Chairman, I appreciate the opportunity to provide this subcommittee with information on the activities of the Program Manager's Office and look forward to your questions. Thank you.

Mr. MCCAUL. Thank you, Mr. Paul, and thank you for recognizing the importance of information sharing, fusion centers.

Mr. Keating, my Ranking Member, we both worked with fusion centers. Sometimes they are given a bit of a bad name, and I think that privacy protection piece is important to preserve the integrity of the work that they are doing and to make sure that privacy interests are protected.

So, with that, I again want to focus back to what this hearing is all about, and that is Fort Hood.

Now, my question may go outside of your expertise or ability to comment. But, again, in this case I think you had a huge breakdown in information sharing, not only between the FBI within

[2] *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") (November 2006) available at *http://ise.gov/sites/default/files/PrivacyGuidelines20061204_1.pdf*.

itself but also with the Department of Defense. If you can speak to these issues, I would like to know how to fix this.

First, you have got an agent sitting at WFO who sits on this matter for the maximum amount of time possible, looks at the lead on the very last day. I understand the FBI is swamped. They have a lot on their plate. But when you have a major at Fort Hood who is the subject matter, I think that would take a little higher priority. But they wait until the very last day and within 4 hours make an analysis based upon two of 18 emails because this analyst doesn't know how to access the database that would give him the other 16 emails, one of which, as I mentioned previously, telegraphs what he is getting ready to do. So you have got that breakdown.

Then, you know, finally, within these task forces you actually have Department of Defense representatives. Why on either side, both from Washington or San Diego, in your opinion—and maybe you can't speak to this—but why didn't one of those DoD representatives on the JTTFs contact Fort Hood and say, you got a problem?

Mr. PAUL. Commenting on the specific operational aspects of Fort Hood are a little bit outside of my lane.

But what I would like to come to is some of the comments that were discussed on the earlier panel that relate to this question, things like doing a better job of enterprise data management. That was a key recommendation coming out of the Webster Commission. It is a key focus of my office, all right. There is a recognition, this goes back to the 9/11 Commission, a series of seminal reports from the Markle Foundation that is codified in the Intelligence Reform and Terrorism Prevention Act. It is really the mandate for my office. It is to drive a better job of enterprise data management so we can knit together all the different aspects of National and public security to keep the American people safe.

I mean, think about 800,000 police officers in this country. The bulk of law enforcement is State and local, 18,000 police departments. Knitting that together into a coherent National architecture requires a focus on common processes, policies, and data standards.

We have had success with that, actually. I mentioned in my opening comments about the National information exchange model. What is not widely understood is that originated with State and local law enforcement. It is actually a State and local innovation that we have adopted at the Federal level as the basis for our counterterrorism data sharing enterprise.

So I think, you know, the focus on knitting together all these different components into a coherent architecture really is the key.

Mr. MCCAUL. You know, as somebody who has worked on the FISA applications, I understand the restrictions when a FISA is out there, like in this particular case with Mr. al-Awlaki. I think there is so much apprehension when you get in the FISA world and so many restrictions, legal restrictions, that that may have been counterproductive and may have gotten in the way of these Department of Defense employees or officials sharing this information with Fort Hood, which is something that the Ranking Member and I would like to maybe look at jointly as to if we have to reform it or somehow just have some sort of reporting language that would clarify that that can be shared.

I can't imagine why, if the Federal Government has this information within its hands, it can't share it with the United States Army, United States military, you know, on one of its bases. To me, that is just incomprehensible.

So I thank you for your testimony.

With that, I recognize the Ranking Member.

Mr. KEATING. Thank you, Mr. Chairman.

Mr. Leiter and Mr. Winter had said that although the chances would have been less likely, the circumstance, this tragedy at Fort Hood could indeed occur again today. Could you reflect on your thinking whether it could occur today?

Also, what would you give for your recommendations to try and not have—the greatest legacy we can give to these families that have lost loved ones are—I think the greatest legacy is that this wouldn't happen again to another American. Could you comment on what you think in that regard?

Mr. PAUL. It is difficult to answer a hypothetical about the specific events that occurred at Fort Hood. But what I will say, and I will highlight the Nation-wide Suspicious Activity Reporting Initiative, you know, one of the things that we are really successful on with this initiative is being able to bring together a lot of different voices across levels of government, and outside the Government, to identify a process for doing suspicious activity reporting that addressed privacy, civil liberties concerns, but also operational effectiveness. Through that process, we were able to identify 16 behaviors reasonably indicative of terrorism-related activity or preoperational criminal planning. So that functional standard is in place Nationally now.

You know, coming back to the question about policy or things like that, when we started that journey a lot of folks were concerned that we wouldn't be able to rationalize how folks looked at these kinds of issues because of the levels of government and the privacy issues. But we were able to work through those successfully, all right. So I think there is a model there, and I go back to that as——

To answer your question about, you know: What is the highest priority? From where I sit, accelerating responsible information-sharing practices, as championed by my office, you know, is a real part of the answer in terms of dealing with the enterprise data management issues that were highlighted, dealing with the jurisdictional issues, dealing with the cultural issues, I think just accelerating the work.

Mr. KEATING. The other thing that Mr. Leiter mentioned is, when we were talking about a patchwork system versus a National system, he referred to having six regional areas perhaps as an approach that would be effective. What do you think in terms of that?

Because I do think the more you have it under one roof, so to speak, even though it might be an IT roof, the more that is there the better off we are. His reference to having six regional areas as sort of a better step than we have now in this patchwork quilt, do you think that would be effective as well? I mean, you are dealing with getting the same message, but the process by which it is reviewed and shared is the issue, too.@

Mr. PAUL. You know, the Information Sharing Environment by design, by statute is a distributed and decentralized environment that interconnects existing systems. So the focus we have is on interoperability but not just at the technical level. It is not about pipes and things like that. That is an important component, but it is more. It is interoperability at the policy level, the business process level. So we think it is key to keep that focus on interoperability so that you can seamlessly share the information.

Now, the FBI approach on regionalization, that is a focus on coordinating Federal activity, which I think is a good thing. It is something we have heard from our State and local partners. It is something that we are working through the different governance structures.

Mr. KEATING. I will just ask you this, too. We had a hearing in Houston, actually, on the Port of Houston and security. One of the things that came out of that was the need for the first line, the need for local police to be there and to be really one of the most important flash points in terms of information.

I must tell you, it is just my feeling, that of all the areas, we are talking about all the higher governmental areas, Department of Defense, FBI, I just don't see enough effort or enough success at that local level, the front line. Sometimes that information can be just the catalyst to spring the network of information that really will tell us something. What are your recommendations to really do a better job at the local level of having them be part of that information network?

I know there is agencies that don't want to go down to that level for fear that some of that information might be breached. But the other side of that is, without sharing that information at the local level, you could really lose probably the most important information that you could have in front of you in the most time-sensitive way.

Mr. PAUL. You know, we have had some success as a Government with the National network of fusion centers and their increasing maturity. Those efforts are led by DHS with close involvement from FBI—integral involvement from FBI, and DOJ, and other Federal agencies.

I talked about the SAR initiative before. Three hundred thousand police officers in this country have been trained. It is the first time that I know of where these police officers have been through the same training. It was around the behaviors I mentioned earlier.

So there is some success that way. It's at risk right now because of the fiscal situation, right?

This goes to—you know, to answer your question, when I talk to my State and local stakeholders, that comes back loud and clear. When you look across that landscape, 18,000 police departments, 90 percent of which have 50 or fewer sworn officers, there is a real concern about the smaller departments, which make up the bulk of law enforcement, how to integrate them in the National architecture. So a focus of our office and working with our stakeholders is to look at solutions like regionalization, you know, that is controlled by States, or State-wide information-sharing environments, or co-location. All right. There is a variety of different approaches, and they are talked about in the annual report.

But I think thoughtful solutions like that to help bring people together to have a common information infrastructure are a key part of dealing with this financial issue as well as knitting together the smaller departments into a National architecture.

Mr. KEATING. So, just to be clear, you are hearing from the local stakeholders that they are saying that if there was, for instance, Federal money that could go to that kind of training, then they would be more apt to participate and then be a part of this, you think, from their vantage point?

Mr. PAUL. When I talk to the State and locals and the Federal, there is a key focus on making sure that as we have these investments today, right, in the fusion centers and in other initiatives that we are looking at making them as effective as possible by expanding the usage of them with the smaller agencies and also looking at, over time, other priority crimes, other priority threats that allow then the business case to be made more effectively for these and to develop support for them.

Mr. KEATING. Okay. Thank you. I yield back.

Mr. MCCAUL. The gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman.

Mr. Paul, thank you for your work. Your vision and your goal for information sharing that will help prevent future attacks on this country and just help law enforcement in general and mine are similar, are shared, really. So I thank you for the work.

In subsequent hearings or past hearings, we have talked with all the agencies, DHS, State, about information sharing between those agencies. Some of the things that I have learned is that if someone—and I will use the case of maybe a visa overstay, and DHS was looking into someone who may or may not overstay their visa and investigate the background of that person. Sometimes they have to come out of one database or system and actually log into another and come out of that system and actually log into another. I even heard that an MS–DOS-type program or database is still being used. I hadn't even heard the word DOS in so many years that that kind of caught me by surprise.

But they are all passwords, entry level. So instead of having one password or one biometric system where one person could enter one time and get in all the databases that they need, they are having to remember all the different passwords. That gets frustrating, and they end up not doing a complete search because of the frustration level.

So I just share that with you, because I think you need to know that. That is what I am hearing from people that currently work in the different levels of government.

In your prepared statement, you talked about the transformation of information ownership to information stewardship, which I think that is a very valid point. Do you believe we have reached that point of information stewardship? In my experience, there are still holdouts today, 11 years after 9/11, 3 years after Fort Hood, where folks refuse to partner or share their information. They still consider they have got ownership of that, and they really don't want to share it for whatever reason, whether they want to hold themselves up to their superiors as the person in the know or the person that has the ability to move up in the ranks. We see that in the

private sector as well. How do we overcome that? Are we overcoming that? What do you foresee in the future?

Mr. PAUL. Thank you. That is a focus of the work of my office, and I appreciate you mentioning the stewardship focus. It has taken us a long time as a Government to develop the siloed structures, the programmatic structures, and we have lots of policies around information that is based on classes of information and that is specific to agencies or bureaus.

The vision that I talked about that Director Clapper talked about is more focused on policy around classes of decisions. The Markle Foundation called it an authorized use standard. It is a big job to look at the body of policy we have and how do we transition it to making decisions about information sharing, discoverability, and things like that based on the classes of decisions. It requires the technical infrastructure, right, with networks that are secure, where identity management works across these networks, across different organizations, across different levels of government, where we have more consistency in how we implement policy in the computer systems.

This is a lot of work. It is a big journey in front of us.

We have had some successes. You know, one that I will mention is related to the watch list that Mr. Leiter was talking about earlier is a success. When somebody gets stopped by State and local law enforcement and there is a hit on the watch list, we have a process now where that information gets back to the local fusion centers and the Joint Terrorism Task Forces in a timely manner. All right. So that is important again to bring in State and local law enforcement into having that situational awareness of what is going on in their communities.

So there is more processes, more work to do, but it is a valid point, and it is where we are headed is the stewardship focuses.

Mr. DUNCAN. I applaud the fusion centers. I see it as the first platform, as long as those platforms are integrated to talk to the higher platforms, so that the higher-up authorities have the ability to go to one platform and be able to Google, so to speak—to use that term not necessarily, that company—but your name and find out everything that someone at a decision-making level needs to know about you. So I applaud your work.

I appreciate this committee, the questions that have been raised here. Mr. Chairman, I really don't have anything else.

Mr. MCCAUL. I thank the gentleman.

The gentleman from Illinois, Mr. Davis, is recognized.

Mr. DAVIS. Thank you very much, Mr. Chairman; and thank you, Mr. Paul, for your testimony.

Government-wide there have been challenges to the development of unclassified and classified systems of information sharing. In particular, DHS has had problems in the past developing and deploying these information-sharing systems.

Let me ask you, how will the recent round of cuts to the budget impact development of some of these systems? How can we make sure that they are developed and get to the State and local and Tribal governments that need them?

Mr. PAUL. It is difficult for me to comment on the cuts specific to DHS, but I do want to highlight that DHS, with their classified

network, the HSDN system, has connectivity out to the fusion centers, and they have been making some stellar progress with the HSIN system, Homeland Security Information Network.

We are also doing a lot of work to drive interoperability across DHS's HSIN system, FBI's LEO—Law Enforcement Online—the IntelLink system out of the intelligence community, and also the grant-funded, State-owned Ris.Net.

So that is a core initiative of the office, is to have interoperability. Our philosophy—there is no wrong door. When you are in a fusion center, working in a police department, line law enforcement, you can get into these systems and find the information.

We have made progress, as I talked about in the Annual Report, but I don't want to overstate that. There is still a lot of work to do there.

We do think that having consistent standards and architecture and working with industry to make sure that we are not building systems and then trying to interconnect them in a one-off manner, that kind of a jerry-rigged approach is not the right way. The right way is to have a consistent architecture that is used across these different systems and by our State and local partners and work with industry and standards organizations to make sure that, you know, identity management is done in a consistent, best practices way, that we are implementing access-based authorization and controls that people can discover information. I think that it is a challenge, there is more work to do, but we have made some substantial progress.

I do want to highlight that key to making this progress is the fact that we have integrated our State and local stakeholders into our governance structures. We do that both—in a variety of ways, but in particular we focus on working with professional associations. That gives us a big ability to help drive culture change, because it is bottoms-up, and it is inclusive.

Mr. DAVIS. Let me ask you, it is my understanding that the eGuardian system set up by the FBI is a major part of the National Suspicious Activity Reporting, or SAR, Initiative and is the main way that State and local law enforcement can share information on suspicious activities with one another and with the Federal Government. How helpful has this system and has SARs in general been for Federal counterterrorism efforts? Can you give an estimate of how many State and local law enforcement SARs have led to Federal counterterrorism investigations?

Mr. PAUL. The Suspicious Activity Reporting Initiative is foundational to our domestic counterterrorism activities. It is a critical integral part. There is approximately 20—maybe a little bit more now—I can give you the precise numbers after the hearing—in the suspicious activity reports that have been vetted to the functional standards that my office has published. There is something on the order of 40,000 searches in what is called a Shared Space. That is the electronic pool, if you like, that the fusion centers and the Joint Terrorism Task Forces and other participants in the ISE use to share this information.

Numerous cases have been opened by the FBI. I believe those numbers are for official use only, so I would like to respond for the record or in a different way for those numbers.

You know, the eGuardian system is one of two technologies. The other is what is called Shared Space. They are interoperable. The important thing is they work within the functional standard, and there is a common process for how the information flows from the citizenry, from industry, critical infrastructure, key resource sectors, to local law enforcement, to the fusion centers, and the Joint Terrorism Task Forces, shared for analytic purposes.

Mr. DAVIS. I would just suspect that the number—or that there would be some serious increase in the reporting of suspicious activity.

Mr. PAUL. There is a substantial number, a substantial number of investigations that are across this Nation related to suspicious activity reporting, either directly out of the SAR system or SAR-like activity. It is foundational.

Mr. DAVIS. Thank you very much.

I have no further questions, Mr. Chairman. I yield back.

Mr. MCCAUL. I thank the gentleman.

Mr. Paul, let me thank you for your testimony as well.

I just want to conclude by saying that we have representatives of the victims and their family members here today at this hearing, and I think the Federal Government deserves—or should give an apology, a formal apology as to what happened, and should call this what it actually was. It was an act of terrorism, and I do believe that the families of the victims need to be compensated adequately and given our deepest respect. As for this Member of Congress and this committee, you have my assurance that we will do everything we can to make sure that that happens.

So, with that, the hearing record will be open for 10 days.

Without objection, this committee is adjourned.

[Whereupon, at 11:01 a.m., the subcommittee was adjourned.]