Douglas E. Winter
Bryan Cave LLP

Deputy Chair, The William H. Webster Commission
on the
Federal Bureau of Investigation, Counterterrorism Intelligence,
and the Events at Fort Hood, Texas, on November 5, 2009

WRITTEN STATEMENT

before the
Subcommittee on Oversight, Investigations, and Management
of the U.S House of Representatives Committee on Homeland Security

"Lessons from Fort Hood: Improving Our Ability to Connect the Dots"

September 14, 2012
311 Cannon House Office Building
Washington, D.C.

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-Aulaqi (sometimes spelled "Awlaki"). He sent a message to Aulaqi. 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 Aulaqi, 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, D.C., 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 meantime, San Diego had acquired and reviewed twelve additional messages and emails from Hasan to Aulaqi and two emails from Aulaqi 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 Aulaqi on June 16, 2009. Aulaqi 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-Aulaqi 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 Aulaqi; 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 seven 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 Aulaqi 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-Aulaqi

In early 2009, the FBI knew Anwar al-Aulaqi as an English-speaking, anti-American, radical Islamic cleric and the subject of an FBI counterterrorism investigation. San Diego believed that Aulaqi was developing ambitions beyond radicalization. WFO viewed him as merely inspirational. The FBI's full understanding of Aulaqi'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 five months as San Diego acquired and reviewed fourteen further messages from Hasan to Aulaqi and two emails from Aulaqi 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 U.S. 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

Aulaqi investigation, thus believed that, if the sender was in fact Hasan, he might have access to IIRs. To protect the Aulaqi 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 Aulaqi 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 fifty 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 ninety days of assignment.

WFO-SSA assigned the lead to a DCIS Agent detailed to the JTTF (WFO-TFO). WFO-TFO waited ninety days – until May 27, 2009, the day his work on the lead was supposed to be completed – to read it and take action. The ninety-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 four hours on that ninetieth 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, D.C., area, WFO-SSA and WFO-TFO treated Hasan as part of San Diego's investigation of Aulaqi. 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-Aulaqi 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 Aulaqi were benign and acceptable. They also erred in failing to search the database in which electronic communications were stored, if only to determine whether Aulaqi 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 Aulaqi.

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 Aulaqi 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-Aulaqi 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 five 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 Aulaqi'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 Aulaqi 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 fifty-day delay in the assignment of the lead and the ninety-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 Aulaqi 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 Aulaqi-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 Aulaqi 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-Aulaqi communications in isolation as eighteen 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 Aulaqi. 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 eighteen (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 Other Large-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)