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

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
Deputy Chair and Editor-in-Chief

Adrian L. Steel, Jr.
Governing Authorities Liaison

William M. Baker

Russell J. Bruemmer

Kenneth L. Wainstein

Adjutant

Stephen J. Cox

Associates

George F. Murphy
Margaret-Rose Sales

With special thanks to Jerrold M. Post, M.D.,
Jane C. Anundson, Barbara J. Fisher, Laura Green, Clara E. Helbringer,
Alicia M. Kartorie, Joan M. McCoy, Janie A. McCutchen, and Barbara Raffaele

COMMISSION BIOGRAPHIES

William H. Webster served as Director of the Federal Bureau of Investigation from 1978 to 1987, and as Director of Central Intelligence from 1987 to 1991. He also served as U. S. Attorney for the Eastern District of Missouri from 1960 to 1961 and as U.S. District Judge for that District from 1970 to 1973. In 1973, Judge Webster was elevated to the U.S. Court of Appeals for the Eighth Circuit, a position he held until 1978. Judge Webster is a graduate of Amherst College and Washington University Law School. He served as a Lieutenant in the U.S. Navy in World War Two and the Korean War. Judge Webster is a retired partner in the law firm Milbank, Tweed, Hadley & McCloy.

Commissioners

Douglas E. Winter is Of Counsel and a former partner in the law firm Bryan Cave LLP, where he is Head of the firm's Electronic Discovery Unit. He specializes in complex litigation and investigations, information technology and review, and records management. He served as law clerk to Judge William H. Webster on the U.S. Court of Appeals for the Eighth Circuit from 1975 to 1976. He served as a Captain in the U.S. Army. Mr. Winter is a graduate of the University of Illinois, Harvard Law School, and the U.S. Army Judge Advocate General School.

Adrian L. Steel, Jr. is a partner in the law firm Mayer Brown LLP, where he served as Chair of the firm's global Pro Bono Committee from 2005 to 2011. His primary practice involves antitrust and regulatory law. He served as a Special Assistant to Director William H. Webster at the Federal Bureau of Investigation from 1978 to 1981. He also served as a law clerk to Judge Webster on the U.S. Court of Appeals for the Eighth Circuit from 1975 to 1976. Mr. Steel is a graduate of the University of Missouri-Columbia and the University of Michigan Law School.

William M. Baker, a consultant, retired from the Federal Bureau of Investigation in 1991. As Assistant Director, Criminal Investigative Division, he was responsible for all FBI criminal investigations, including counterterrorism. He also served as the FBI Assistant Director of Congressional and Public Affairs, and as Director of Public Affairs at the Central Intelligence Agency from 1987 to 1989. He was Senior Vice President of the Motion Picture Association of America and then President of its international arm from 1991 to 2000. Before joining the FBI, he served as a Lieutenant in the U.S. Air Force Office of Special Investigations. Mr. Baker is a graduate of the University of Virginia.

Russell J. Bruemmer is a partner in the law firm WilmerHale, where he is Chair of its Financial Institutions Group. He served as Special Counsel to Director William H. Webster at the Central Intelligence Agency and as the CIA's General Counsel from 1987 to 1990. He served as Special Assistant to Director Webster at the Federal Bureau of Investigation from 1978 to 1980, and FBI Chief Counsel-Congressional Affairs from 1980 to 1981. He also served as law clerk to Judge Webster on the U.S. Court of Appeals for the Eighth Circuit from 1977 to 1978. Mr. Bruemmer is a graduate of Luther College (Iowa) and the University of Michigan Law School.

Kenneth L. Wainstein is a partner in the law firm Cadwalader, Wickersham & Taft LLP, with expertise in corporate internal investigations and civil and criminal enforcement actions. He served as FBI General Counsel and Chief of Staff to Director Robert S. Mueller II (2002-2004); the first Assistant Attorney General for National Security (2006-2008); and Homeland Security Advisor to the President (2008-2009). He has been U.S. Attorney for the District of Columbia (2004-2006); Director of the Executive Office for U.S. Attorneys (2001-2002); and an Assistant U.S. Attorney in the Southern District of New York and the District of Columbia (1989-2001). Mr. Wainstein graduated from the University of Virginia and the Law School of the University of California at Berkeley. He served as law clerk Judge Thomas Penfield Jackson of the U.S. District Court for the District of Columbia.

Adjutant

Stephen J. Cox is Corporate Counsel at Apache Corporation. He is a former senior associate at WilmerHale, where his practice focused on Congressional investigations, crisis management, litigation, and regulatory affairs. He served as a law clerk to Judge J. L. Edmondson on the U.S. Court of Appeals for the Eleventh Circuit from 2006 to 2007 and as Advisor to the Assistant Secretary of U.S. Immigration and Customs Enforcement from 2007 to 2008. Mr. Cox is a graduate of Texas A&M University and the University of Houston Law Center.

Associates

George F. Murphy is an associate in the Washington, D.C., office of the law firm Bryan Cave LLP. His practice involves white collar criminal defense and investigations and international trade. He has served on the Advisory Board of the Children's Law Center since 2010. Prior to practice, he served as a law clerk for the Appellate Defense Division of the U.S. Navy Judge Advocate General's Corps. Mr. Murphy is a graduate of Brown University and George Washington University Law School.

Margaret-Rose Sales is an associate in the Washington, D.C., office of the law firm Mayer Brown LLP. She practices in the Government and Global Trade Group. Ms. Sales worked earlier at U.S. Customs Border Protection, Department of Homeland Security. She is a graduate of McGill University, Georgetown University, and Georgetown University Law School.

TABLE OF CONTENTS

Introduction

On December 17, 2008, United States Army Major Nidal Malik Hasan visited the website of radical Islamic cleric Anwar al-Aulaqi. He sent a message to Aulaqi. The Federal Bureau of Investigation acquired the message. A second message followed on January 1, 2009. Members of the Joint Terrorism Task Force (JTTF) in the San Diego Field Office reviewed the messages. Concerned by the message's content and implications that the sender was a U.S. military officer, San Diego set a lead to International Terrorism Operations Section 1 at FBI Headquarters and the JTTF in the Washington, D.C., Field Office (WFO).

Five months later, WFO conducted an assessment of Hasan, who worked as a psychiatrist at the Walter Reed Army Medical Center. WFO queried certain FBI and Department of Defense (DoD) databases and reviewed the limited set of Army personnel records available to DoD personnel serving on JTTFs. In the meantime, San Diego had acquired and reviewed fourteen additional messages and emails from Hasan to Aulaqi and two emails from Aulaqi to Hasan.

WFO did not assess Hasan to be involved in terrorist activities. San Diego advised WFO that the assessment was inadequate. Neither Field Office took any further action. Hasan sent his last message to Aulaqi on June 16, 2009. Aulaqi did not respond.

Effective July 15, 2009, the Army assigned Hasan to the Darnall Army Medical Center at Fort Hood, Texas. In October 2009, the Army notified Hasan that he would be deployed to Afghanistan in November 2009.

On November 5, 2009, Hasan entered the Fort Hood deployment center. He carried two pistols. He jumped on a desk and shouted "Allahu Akbar!" – Arabic for "God is great!" Then he opened fire, killing twelve U.S. soldiers and one DoD employee, and injuring forty-two others.

The FBI immediately conducted an internal review of how San Diego and WFO handled Hasan's communications with Aulaqi. As a result of the review, the FBI took specific steps to improve its ability to detect and deter threats like Hasan. Those steps focused primarily on FBI-DoD information-sharing, FBI Headquarters involvement in reviewing significant national security cases, information technology improvements, and training.

FBI Director Robert S. Mueller, III, determined that an additional, independent investigation of the FBI's actions was appropriate.

A. The Terms of Reference

On December 17, 2009, Director Mueller asked William H. Webster, a former U.S. Attorney, U.S. District Judge, U.S. Circuit Judge, Director of the FBI, and Director of the Central Intelligence Agency, to conduct an independent investigation of the FBI's handling of the Hasan information. Without limiting the investigation, Director Mueller's Terms of Reference asked Judge Webster to examine:

(1) the laws and policies applicable to the FBI's assessment of the threat posed by Major Hasan;

(2) whether the FBI complied with applicable laws and policies;

(3) whether the actions taken by the FBI were reasonable under the circumstances known at the time, and, if not, whether any administrative action should be taken against any employee;

(4) whether current laws and policies strike an appropriate balance between protecting individuals' privacy rights and civil liberties and detecting and deterring threats such as that posed by Major Hasan;

(5) whether the steps the FBI is taking following an internal review of the shooting are sufficient or whether there are other policy or procedural steps the FBI should consider to improve its ability to detect and deter such threats in the future; and

(6) whether the FBI should propose any legislative action to improve its ability to detect and deter such threats while still respecting privacy and civil-liberty interests.

B. The Investigation

Judge Webster assembled a team of seasoned investigators and attorneys to assist him. The FBI provided the Webster Commission with unfettered access to personnel, documents, and technology. An FBI liaison assisted in scheduling briefings, interviews, and Field Office visits, and in identifying and producing FBI, Department of Justice (DOJ), DoD, and other government documents. The FBI and the DOJ provided the Commission with more than 50 formal interviews, meetings, and briefings; a far greater number of informal briefings and meetings; and more than 300 documents totaling more than 10,000 pages. The FBI's Special Technologies and Applications Section provided Commission members with direct access to FBI computer systems, applications, and databases.

The Commission or its specialized teams conducted investigative interviews of all FBI and other JTTF personnel who handled the Hasan information; conducted on-site visits and interviews with counterterrorism squads and intelligence fusion cells in Northern Virginia, Philadelphia, and Los Angeles that were not involved in the Hasan matter; and performed or supervised comprehensive searches of the FBI's data holdings on Hasan and Aulaqi. To obtain a broad range of perspectives, the Commission also consulted with outside experts on

counterterrorism, intelligence operations, information technology, and Islamic radicalism; public interest groups that promote and protect civil liberties and privacy interests; and staff from Congressional committees with FBI oversight responsibilities. The input of more than 300 persons informs our investigation and recommendations. We also reviewed hundreds of non-government documents relevant to our inquiries.

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 this Report reviews the specifics of one tragic event, it also speaks to transcendent issues that are crucial to the FBI's ability to combat terrorism in the electronic age.

Part One of this Report presents our Factual Findings. Chapters 1 and 2 discuss the challenge of violent radicalization and one of the FBI's primary responses, the Joint Terrorism Task Force program. Chapters 3 and 4 review the legal, operational, and technological framework for the FBI actions at issue. Chapter 5 describes the FBI's investigation of Anwar al-Aulaqi. Chapter 6 describes the FBI's actions in connection with the Hasan-Aulaqi communications. Chapter 7 summarizes our review of the FBI's data holdings to identify what information about Hasan and the Hasan-Aulaqi communications was available to the FBI before and after the Fort Hood shootings.

Part Two contains our Analysis of the reasonableness and adequacy of the FBI's actions in the context of the governing authorities, FBI policies and practices, and the operational and technological environment of the time.

Part Three assesses the adequacy of the remedial steps that the FBI took following its internal review of the Fort Hood shootings.

Part Four considers whether the FBI's governing authorities properly balance civil liberties and privacy interests with the FBI's counterterrorism obligations. It also discusses the potential evolution of those authorities.

Part Five contains our Recommendations for additional improvements to enhance the FBI's ability to fulfill its counterterrorism mission and make our country a safer place to live while respecting civil liberties and privacy interests.

C. FBI/U.S. Intelligence Community Personnel Identifiers

At the FBI's request, this Report identifies FBI and other U.S. Intelligence Community personnel by anonymous abbreviations that indicate each person's geographic location or headquarters assignment and job title.

San Diego Field Office/Joint Terrorism Task Force

FBI Supervisory Special Agent	SD-SSA
FBI Special Agent	SD-Agent
FBI Intelligence Analyst	SD-Analyst
Task Force Officer 1 (NCIS)	SD-TFO1
Task Force Officer 2 (NCIS)	SD-TFO2
Task Force Officer 3 (DCIS)	SD-TFO3

Washington, D.C., FBI International Terrorism Operations Section 1

FBI Supervisory Special Agent	ITOS1-SSA
FBI Special Agent	ITOS1-Agent
FBI Intelligence Analyst	ITOS1-Analyst

Washington, D.C., Field Office/Joint Terrorism Task Force

FBI Supervisory Special Agent	WFO-SSA
FBI Intelligence Analyst	WFO-Analyst
Task Force Officer (DCIS)	WFO-TFO

Department of Defense, Defense Criminal Investigative Service

DoD Intelligence Analyst	DCIS-Analyst

An Index of all acronyms used in this Report is appended.

D. FBI/U.S. Intelligence Community Redactions

This Final Report reviews sensitive counterterrorism intelligence and other classified information. The FBI National Security Legal Branch, in cooperation with other members of the U.S. Intelligence Community, has redacted that classified information – and only that information – from the public version of the Final Report. The public version includes, to the extent possible, unclassified descriptions of the content of those redactions. [Those descriptions, like this sentence, appear in brackets.]

Part One

Factual Findings

Chapter 1

Violent Radicalization

A. Introduction

The Fort Hood shootings are a grim reminder that violent radicalization is a persistent threat to the United States and its citizens and residents. Radicalization – whether based on religious, political, social, or other causes – challenges the capability and capacity of the FBI and other members of the U.S. Intelligence Community to identify, collect, analyze, and act on accurate intelligence in time to detect and deter those who would commit violence.

> Although highly publicized terrorist plots and acts – and the Fort Hood shootings – have referenced Islam, violent radicalization transcends any one religion – and, indeed, religion – and can find causes in political, social, environmental, and other contexts. The FBI's report on terrorist acts in the U.S. between 1980 and 2005 identified 318 events (including bombings, arson and malicious destruction, and shootings); only 7% of those events were attributed to Islamic extremists. Federal Bureau of Investigation, *Terrorism 2002–2005* (2d ed. 2007).

Radicalism is not a crime. Radicalization alone, without incitement to violence, may not constitute a threat. Our Constitution protects thoughts, words, and even actions associated with extremism, including speeches, public assemblies, and attendance at places of worship. There are limits, of course. The First Amendment, for example, does not embrace language that can cause objective harm to people, their possessions, or their liberties. The Constitution does not shield those who, in pursuit of radical ends, would cause harm – or those who incite or support those who would cause harm.

In a 2006 speech, FBI Director Mueller observed that understanding radicalization and countering its violent ends require constant calibration of how the FBI understands "the line between the extremist and the operational." See Director Robert S. Mueller, III, *The Threat of Homegrown Terrorism*, Speech to The City Club of Cleveland (June 23, 2006). In the age of electronic communications, that line can be difficult to discern.

Nidal Malik Hasan's transformation into a killer underscores the dilemma confronting the FBI. Hasan was a licensed psychiatrist and a U.S. Army Major with fifteen years of military service. He was a member of two professional communities – mental health and defense – whose missions include protection against violence. He worked at Walter Reed Army Medical Center and other facilities in close and constant contact with other U.S. military personnel, including fellow psychiatrists. He was a religious person. He had no known foreign travel. Other than his eighteen communications with Anwar al-Aulaqi, he had no known contact and no known relationships with criminal elements, agents of foreign powers, or potential terrorists.

This Report considers a myriad of factors that affect the FBI's ability to detect – and, when legally possible, deter and disrupt – the violent radicalization of U.S persons. These factors include the FBI's legal authority, written and informal policies, operational capability and capacity, access to information, and technology. In this Chapter, we examine the pre-eminent factor: the FBI's understanding of violent radicalization.

We spoke with FBI counterterrorism officials, as well as Agents, Analysts, and Task Force Officers at FBI Headquarters and in the field, to examine the FBI's understanding of violent radicalization and its implications for intelligence, operations, and training before and after the Fort Hood shootings. We consulted in unclassified settings with Jerrold Post, M.D., Professor of Psychiatry, Political Psychology, and International Affairs at George Washington University. (Dr. Post served 21 years with the Central Intelligence Agency, where he founded and directed the CIA's Center for the Analysis of Personality and Political Behavior. The CIA awarded Dr. Post the Intelligence Medal of Merit in 1979 and the Studies in Intelligence Award in 1980. He is a Life Fellow of the American Psychiatric Association, and the Association's Chair of the Task Force for National and International Terrorism and Violence.) We also reviewed contemporary learned texts to examine the psychiatric community's understanding of violent radicalization and the role of the Internet in violent radicalization.

B. The Process of Violent Radicalization

1. The Dynamics of Violent Radicalization

The psychiatric community has identified the fundamental dynamics of violent radicalization:

(a) Most terrorists are psychologically normal as individuals, and do not fit a medical diagnostic category.

(b) Radicalization is not precipitous, but a process with "many way stations...."

(c) Violent radicals are creatures of a collective identity. Group, organizational, and social psychology – not individual psychology – provide the most powerful insights on terrorist behavior. (Indeed, group psychology plays an integral role in "self-radicalization" as well as "lone wolf" terrorism.)

(d) Leaders are essential to radicalization. Leaders draw together alienated, discontented, and isolated followers who are prone to or ready to accept a collective identity.

(e) Radicalization occurs when followers submit to the collective identity and leaders identify a shared enemy as a target for violent behavior.

(f) Radicalization involves "a continuing reinforcement by manipulative leaders, consolidating collective identity, externalizing, and justifying ... [and then] requiring violence against the enemy."

J.M. Post, et al., *The Psychological and Behavioral Bases of Terrorism: Individual, Group and Collective Contributions*, 14 INT'L AFF. REV. 195, 196-99 (Fall 2005).

2. The FBI Model

In 2007, the FBI published a model of violent radicalization that parallels the understanding of the psychiatric community. See C. Dyer et al., *Countering Violent Islamic Extremism*, FBI LAW ENFORCEMENT BULLETIN, Dec. 2007.

The FBI model describes the process of violent radicalization – the "way stations" – as four incremental stages of development:

Preradicalization → Identification → Indoctrination → Action

"Pre-radicalization" is measured by an individual's motivation, stimuli, and opportunity to radicalize. C. Dyer et al., at 6. A motivation for conversion – whether to a religion or another cause – is critical to the process, and can take several forms.

"Acceptance seeking" conversions are a product of human nature – the need to form and maintain interpersonal relationships. Persons with limited or fragile social ties may find acceptance in the solidarity of extremist groups. In "jilted-believer" and "faith reinterpretation" conversions, persons frustrated or dissatisfied with a belief system embrace a more militant system. In "protest" conversions, the individual rebels against, or seeks an identity separate from, family, society, or circumstances.

Stimulus is typically provided by a respected leader whose words, actions, or public persona inspire conversion. The opportunity to radicalize ordinarily involves exposure to the commitment of others to the leader or the cause. Differing venues can provide stimulus and opportunity, including prisons, places of worship, universities, private settings, and the Internet.

The second phase of radicalization, "Identification," is marked by acceptance of and devotion to the cause. C. Dyer et al., at 6. Accepting the cause often leads converts to become isolated from their former lives as they seek guidance from the leader or other followers about how to become more committed to the cause. Social interaction with other followers and travel to live near or within the group may accelerate the process.

"Indoctrination" involves a conviction that the cause requires violent action. C. Dyer et al., at 6. It commonly occurs through active participation in or access to the cause's activities and inner workings. Converts assert a personal stake in the cause and believe that action is needed to support the cause. In religious contexts, extremist clerics can play a major role in indoctrination because of their emotional hold over impressionable followers and their ability to provide spiritual justification for violence.

"Action" is the manifestation of a commitment to engage in violence. C. Dyer et al., at 6. Action can be violent or nonviolent (for example, financing or facilitating others who pursue violence); but its purpose is to further the cause and to harm the perceived enemy.

Radicalization to the final stage is not inevitable. The process of radicalization can be interrupted. The process can be reversed. Many persons reach only the first or second or third stage, without ever entering the stage of action.

The objective of the FBI model is to "identify [through each stage] indicators of those who demonstrate the potential for violence," and the "patterns and trends of extremist behavior." C. Dyer et al., at 4, 8. The challenge lies in finding actionable indicators in time to respond in a lawful manner to the potential for violence. Reliable indicators of radicalization are more difficult to detect and act on in nascent stages. The early phases of radicalization may take place outside the knowledge of anyone but the radicalizing individual. They may also take place in ways that implicate the civil liberties and privacy interests of U.S. persons, cautioning or demanding investigative restraint. Even if the FBI obtains intelligence evidencing an individual in the radicalization process, that intelligence may not provide a legitimate basis for investigation. A person's opportunity to radicalize – for example, by downloading an audio file of a radical speech or sermon – is alone not a justification for investigation. An individual's acceptance of a cause – for example, by joining a peaceful demonstration against Israeli settlements in Palestine – is alone not a justification for investigation. Even an individual's conviction that a cause requires action – for example, by writing an op-ed article in support of Hamas – may not provide a justification for investigation, if that individual shows no inclination to take violent action based on that conviction.

The difficulties of detecting violent radicalization and justifying FBI intervention are exacerbated because the four stages of radicalization progress with ever-increasing speed. Pre-radicalization and identification may take years. Indoctrination and action may take months, weeks, even days. Detection in the early stages may be impossible. Detection in the later stages may not allow time to respond before violence occurs.

3. The Lone Actor and Internet Radicalization

Newspaper reports recently quoted President Obama as stating that "the most likely scenario that we have to guard against right now ends up being more of a lone wolf operation than a large, well coordinated terrorist attack." Associated Press (August 17, 2011). For nearly a decade, the FBI has forecast the dangers of "lone wolf" terrorists, both international and domestic. See The FBI Strategic Plan 2004-2009; Testimony of Patrick Rowan, FBI Acting General Counsel, before the House Perm. Sel. Comm. on Intelligence (July 23, 2003).

Lone actors can pass through the four stages of radicalization with little or no personal contact with a leader or another violent radical – and thus without conventional accomplices, co-conspirators, or handlers. Evolving communications technologies – most notably, the Internet – play an increasingly weighty role in the phenomenon of the lone actor. Radical voices can provide leadership via the Internet at each stage of radicalization, including a call to action for

individuals who have no other association with them. For example, the al-Qaeda Internet treatise *Iraqi Jihad, Hopes and Risks* was the apparent inspiration for the 2004 Madrid train bombings.

The Internet can provide individuals with remote, yet regular, access to the teachings and instructions of violent radical leaders, supplanting the real-world meeting places traditionally used to radicalize – and traditionally used by the FBI to detect violent radicalization. The Internet also offers exposure to extraordinary amounts of information at little or no cost; the ability to join and participate in virtual networks of like-minded individuals, finding the group identity that is part of radicalization; and, of course, the potential for shrouding identities.

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.

Chapter 2

The Joint Terrorism Task Force Program

The actions under review took place in the context of the FBI's Joint Terrorism Task Force (JTTF) program. The San Diego JTTF identified the first two communications from Hasan to Aulaqi and set a lead on Hasan to the Washington, D.C., JTTF.

The Department of Justice (DOJ) and the FBI developed the JTTF program as a counterterrorism partnership among U.S. law enforcement and intelligence agencies. The FBI and the New York City Police Department established the first JTTF in 1980. By September 11, 2001, there were 35 JTTFs in the U.S. Today, there are 104 JTTFs, including at least one in each of the FBI's 56 Field Offices.

The JTTF program organizes and coordinates federal, state, and local resources in an effort to detect, deter, disrupt, and otherwise respond to the threat of terrorism. Each JTTF is a cell of trained investigators, intelligence analysts, linguists, and other specialists from the FBI and other law enforcement, intelligence, and public safety agencies (including, for example, Immigration and Customs Enforcement, Secret Service, regional transit authorities, state highway patrols, and local police departments). JTTF members engage in surveillance, electronic intercepts, source development, interviews, database analysis, and other investigative techniques. They operate daily in the realm of counterterrorism, facing threats that range from lone actors to international terrorist networks.

The JTTF program's success in combating terrorism is well-documented. JTTFs have played crucial roles in foiling major terrorism plots that include, among others:

- Antonio Martinez (planned attack on military recruiting center in Catonsville, Maryland)
- Mohamed Osman Mohamud (planned attack on tree-lighting ceremony in Portland, Oregon)
- Farooque Ahmed (plot to bomb Metrorail stations in Northern Virginia)
- Shaker Masri (planned travel to Somalia to support al Shabaab)
- Zachary Chesser (planned travel to Somalia to support al Shabaab)
- Mohammed Mahmood Alessa and Carlos Eduardo Almonte (planned travel to Somalia to support al Shabaab)
- Hosam Smadi (plot to bomb office building in Dallas, Texas)

- Michael Finton (plot to detonate bomb outside federal building in Springfield, Illinois)

- James Cromitie (plot to bomb a synagogue and military facility in New York City)

- Khalid Ali-M Aldawsari (attending college on student visa; purchased equipment and chemicals to make an improvised explosive device in Lubbock, Texas)

- Colleen LaRose (recruitment of jihadist fighters to commit murder overseas)

- Abu Khalid Abdul-Latif and Walli Majahidh (plot to attack military recruiting center in Seattle)

- Waad Ramadan Alwan and Mohanad Shareef Hammadi (plot to ship money and weapons in support of al Qaeda in Iraq)

The FBI and its JTTF partners established the National Joint Terrorism Task Force (NJTTF) in 2002 to provide a central forum for sharing terrorism threats and intelligence among federal, state, and local agencies, and to provide program management, oversight, and support for JTTFs. The NJTTF is organized within the FBI Counterterrorism Division and at the National Counterterrorism Center. It has 42 member agencies: 11 Department of Defense agencies; 27 other federal agencies; and four state, regional, or local agencies.

The FBI enters into a Memorandum of Understanding or other formal agreement to define each agency's participation in the program. Under these agreements, the FBI funds the participating agencies' direct expenses, including overtime, vehicles, fuel, mobile telephones, and office costs. JTTF personnel from the participating agencies – who are known as Task Force Officers – carry out their duties subject to the laws, policies, and other authorities that govern the FBI. Our examination of the FBI's actions in the Hasan matter thus begins with a review of those governing authorities.

Chapter 3

The FBI's Governing Authorities

The Terms of Reference asked Judge Webster to examine "the laws and policies applicable to the FBI's assessment of the threat posed by Major Hasan."

A. Primary Authorities

1. The Attorney General

The FBI's primary investigative authority derives from the statutory authority of the Attorney General. See 28 U.S.C. §§ 509, 509A, 510, 533, and 534. The Attorney General delegates that authority, primarily in 28 C.F.R. § 0.85, which provides that the FBI shall "[i]nvestigate violations of the laws ... of the United States and collect evidence in cases in which the United States is or may be a party in interest...." Id.

The FBI has lead investigative responsibility for domestic and international terrorism, which includes, among other things, the unlawful use of force and violence against persons or property to intimidate or coerce a government or civilians in furtherance of political or social objectives. See 18 U.S.C. §§ 2331(1) and (5) (providing the complete definition of "terrorism," including the distinction between domestic terrorism and international terrorism). Within the United States, the FBI's counterterrorism mission includes "the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate." 28 C.F.R. § 0.85(l).

2. Executive Order 12333

The FBI's intelligence-gathering authorities also derive from Executive Order 12333, issued by President Ronald Reagan in 1981 and amended by subsequent administrations. The Executive Order grants the U.S. Intelligence Community – including the FBI – the power to use "[a]ll [lawful] means ... to obtain reliable intelligence information to protect the United States and its interests," while preserving the civil rights, liberties, and privacy of all U.S. persons. Exec. Order No. 12333 at § 1.1 (Dec. 4, 1981), as amended by Exec. Order Nos. 13284 (2003), 13355 (2004), and 13470 (2008). It authorizes the FBI, under the supervision and regulations of the Attorney General, to:

(1) collect (including through clandestine means), analyze, produce and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) conduct counterintelligence activities; and

(3) conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations....

Id. at § 1.7(g). "Foreign intelligence includes information relating to the capabilities, intentions, or activities of ... international terrorists." Id. at § 3.5(e).

This broad authority is balanced by the Executive Order's declaration that "[e]lements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General...." Exec. Order No. 12333 at § 2.3. The Executive Order protects against the misuse of foreign intelligence and guards the privacy of U.S. persons by specifying "that no foreign intelligence collection by [Intelligence Community elements other than the FBI] may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons." Id. at § 2.3(b). A "U.S. person" is a citizen, lawfully admitted permanent resident alien, or corporation incorporated in the U.S. Id. at § 3.5(k).

Executive Order 12333 also requires the FBI and other Intelligence Community members to "use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad." Exec. Order No. 12333 at § 2.4. The choice of technique and its level of intrusiveness are matters of judgment in light of the seriousness of the threat. For more serious threats, more intrusive means may be appropriate.

B. Secondary Authorities

1. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., establishes the process for obtaining judicial approval of electronic surveillance and physical searches to collect "foreign intelligence information." FISA defines "foreign intelligence information" as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or

the security of the United States; or (B) the conduct of the foreign affairs of the United States.[1/]

50 U.S.C. § 1801(e).

To collect foreign intelligence information under FISA's electronic surveillance and physical search provisions, the FBI must provide facts to the Foreign Intelligence Surveillance Court (FISC) establishing probable cause to believe that the target of the surveillance or search is a "foreign power" or "agent of a foreign power." 50 U.S.C. § 1804(a)(3)(A); Exec. Order No. 12333 at § 2.5. To pursue electronic surveillance, the FBI must also show that "the facilities or places at which the electronic surveillance is directed [are] being used, or are about to be used" by the target. 50 U.S.C. § 1804(a)(3)(B). To undertake a physical search, the FBI must show that "the premises or property to be searched is or about to be owned, used, possessed by or is in transit to or from" the target. 50 U.S.C. § 1823(a)(3)(C).

To balance the intrusive nature of surveillance and searches – and to protect the rights of non-consenting U.S. persons – FISA requires "minimization" procedures for the acquisition, retention, and dissemination of information collected through electronic surveillance or physical search. 50 U.S.C. §§ 1801(h), 1821(4). FISA requires the Attorney General to adopt procedures to assure, among other things, that nonpublic information that is not foreign intelligence (as defined in 50 U.S.C. § 1801(e)) or evidence of a crime is not disseminated in a manner that identifies any U.S. person without that person's consent, unless that person's identity is necessary to understand foreign intelligence or assess its importance. In most cases, the FBI follows Standard Minimization Procedures (SMPs) approved by the Attorney General and the FISC. Special minimization procedures apply in certain cases. 50 U.S.C. § 1801(h).

Other sections of FISA provide for pen registers and trap-and-trace devices for foreign intelligence purposes; access to certain business records for foreign intelligence purposes; and reporting requirements. 50 U.S.C. §§ 1841-46, 1861-63, 1871.

1/ FISA defines "international terrorism" as activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—
  (A) to intimidate or coerce a civilian population;
  (B) to influence the policy of a government by intimidation or coercion; or
  (C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

50 U.S.C. §1801(c).

2. National Security Letters

Five statutes authorize the FBI to issue administrative subpoenas known as National Security Letters (NSLs) to obtain limited types of information from third-party custodians without court approval:

(1) the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (telephone and email communication records from telecommunications companies and Internet service providers);

(2) the Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A) (records of financial institutions);

(3) the Fair Credit Reporting Act, 15 U.S.C. §§ 1681u(a) and (b) (lists of financial institutions and consumer-identifying information from credit reporting companies);

(4) the Fair Credit Reporting Act, 15 U.S.C. § 1681v (credit reports in international terrorism cases); and

(5) the National Security Act, 50 U.S.C. § 436 (records involving Executive Branch employees in investigations of improper disclosure of classified information).

Like grand jury subpoenas in traditional criminal cases, NSLs allow the FBI to acquire basic information that can serve as the building blocks of a national security investigation. Unlike grand jury subpoenas, however, NSLs are not issued by a U.S. attorney and are limited to the statutorily specified records. Each NSL statute has discrete standards. To our knowledge, Congress has made no effort to normalize these standards to eliminate confusion and the risk of error. Each statute contains non-disclosure provisions, which, upon certification by a specified government official, restrict the recipient's ability to disclose the NSL. The statutes require the FBI to report information to Congress about its use of NSLs. E.g., 18 U.S.C. § 2709(e).

The FBI has no other statutory authority to issue administrative subpoenas. The Attorney General has delegated the authority to the FBI to issue administrative subpoenas under 21 U.S.C. § 876 and 18 U.S.C. § 3486 for drug program investigations and child sexual exploitation and abuse investigations.

3. The PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the PATRIOT Act, was passed on October 26, 2001, in the aftermath of the September 11 attacks. Pub. L. 107-56, 115 Stat. 272 (2001). The PATRIOT Act vested the FBI with new investigative authorities to combat terrorism, amending, among other things, 50 U.S.C. §§ 1801(b)(1)(c), 1805(c)(2)(B), and 1861-63. Although not all of these authorities are relevant to the FBI's actions under review here, we discuss them because of their importance to the FBI's counterterrorism mission. The PATRIOT

Act also helped eliminate the so-called FISA "wall" between law enforcement and intelligence, which had limited the ability of criminal investigators and intelligence agents to share information.

Section 218 of the PATRIOT Act clarifies that the FBI and other members of the U.S. Intelligence Community have the authority to gather, through electronic surveillance and physical searches, "foreign intelligence information" from U.S. and non-U.S. persons. It amended FISA to require a showing that the acquisition of foreign intelligence information was a "significant purpose" – rather than "the purpose" – of the proposed surveillance or search.

Section 505 of the PATRIOT Act revised the standard for issuing NSLs. As originally enacted, the NSL statutes targeted an "agent of a foreign power." Today, the FBI can issue NSLs if the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment. .

Section 206 of the PATRIOT Act amended FISA to enable the government to conduct "roving" surveillance of targets whose actions thwart FISA surveillance. Previously, national security investigators had to obtain a new FISC order each time the target of electronic surveillance used a different communications service provider. With "roving" authority, the FBI can maintain reasonably continuous surveillance as a target moves from one device to another, which is standard tradecraft for surveillance-conscious terrorists and spies. This change brought FISA in line with the Federal Wiretap Act (also known as Title III), which had authorized roving surveillance in criminal cases since 1986. See 18 U.S.C. § 2518(11). When the FBI implements roving authority under FISA, it must demonstrate to the FISC, normally within 10 days, probable cause that the target is using, or is about to use, the new device. See 50 U.S.C. § 1805(c)(3).[2/]

Section 215 of the PATRIOT Act amended FISA to authorize the FISC to issue orders for the production of the types of records and other tangible things that law enforcement officers and prosecutors historically have been authorized to acquire through grand jury subpoenas. See 50 U.S.C. § 1861. Previously, investigators in national security matters could secure a court order only for limited types of records by showing "specific and articulable facts" that the subject was a foreign power or an agent of a foreign power. Section 215 adopted the standard of "relevance to an authorized investigation." 50 U.S.C. § 1861(b)(2)(A).

To obtain a Section 215 order, the government generally must show that (1) the information is sought for an authorized national security investigation conducted under guidelines approved by the Attorney General; (2) the information sought is relevant to the authorized investigation; and (3) if the investigative target is a U.S. person, the investigation is not based solely on activities protected by the First Amendment. 50 U.S.C. §§ 1861(a) and

---

[2/] Courts have upheld the constitutionality of roving surveillance, rejecting claims that it violates the Fourth Amendment's "particularity" requirement. E.g., United States v. Jackson, 207 F.3d 910, 914 (7th Cir.), vacated on other grounds, 531 U.S. 953 (2000); United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996); United States v. Bianco, 998 F.2d 1112, 1122-23 (2d Cir. 1993); United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992).

(b)(2)(A). The government must adhere to minimization procedures that limit the retention and dissemination of information concerning U.S. persons. 50 U.S.C. §§ 1861(b)(2)(B) and (g).

Section 215 prohibits the recipient of a business records order from disclosing it; but the recipient may challenge its legality and any non-disclosure requirement in court. 50 U.S.C. § 1861(d). To date, no recipient of a Section 215 order has challenged its validity or a non-disclosure requirement.

4. The Intelligence Reform and Terrorist Prevention Act

When FISA was passed in 1978, the likely targets of counterterrorism surveillance were agents of an organized terrorist group like the Red Brigades, the Irish Republican Army, or the Palestinian terrorist organizations of that era. Given the increasing fluidity in the membership and organization of international terrorists, the FBI may not be able to ascertain a foreign terrorist's affiliation with an international organization. Section 6001 of the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) allows the government to conduct surveillance on a non-U.S. person who "engages in international terrorism or activities in preparation therefor" without demonstrating an affiliation to a particular international terrorist organization. Pub. L. 108-458, § 6001, 118 Stat. 3638, 3742 (2004).

Sections 206 and 215 of the PATRIOT Act and Section 6001 of IRTPA were scheduled to "sunset" on December 31, 2009. In May 2011, after an interim extension, Congress extended the provisions until June 1, 2015, without amendment.

5. The Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act of 1994 (CALEA), 47 U.S.C. §§ 1001 et seq., requires telecommunications providers to develop and deploy intercept capabilities in their networks to ensure that the FBI and other U.S. law enforcement agencies can conduct lawful, authorized interception and electronic surveillance pursuant to FISA and U.S.C. Title 18.

CALEA's mandate applies to "telecommunications carriers," which the statute defines as entities "engaged in the transmission or switching of wire or electronic communications as a common carrier for hire [including those that provide] ... commercial mobile service" and any other entities that the Federal Communications Commission (FCC) finds provide a service that replaces a substantial portion of local telephone exchange service and, in the public interest, should be subject to CALEA. 47 U.S.C. § 1001(8).

In 2005, the FCC applied CALEA to providers of facilities-based broadband Internet access services and providers of "interconnected" Voice over Internet Protocol (VoIP) services. The FCC defines "interconnected" VoIP services as those that (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the public switched telephone network. See *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 15008 ¶ 39 (2005). The FCC held that

these services had replaced a substantial portion of local telephone exchange service and that public interest factors supported applying CALEA to these providers. Id. at 15001-12 ¶¶ 24-40.

CALEA imposes "assistance capability requirements" on telecommunications carriers to ensure that, in the event of court-ordered or other lawfully authorized government electronic surveillance, these carriers are capable of:

(1) Expeditiously isolating and enabling the government to intercept all wire and electronic communications of a target concurrent with their transmission;

(2) Expeditiously isolating and enabling the government to access reasonably available call-identifying information contemporaneously with its transmission in a manner that allows that information to be associated with the communication to which it pertains;

(3) Delivering intercepted communications and call-identifying information to the government; and

(4) Facilitating interception and access to call-identifying information unobtrusively and with a minimum of interference to the subscriber's service, and in a manner that protects the privacy and security of communications and call-identifying information not authorized to be intercepted and information about the fact of the interception.

47 U.S.C. § 1002(a).

CALEA also requires "manufacturers of telecommunications transmission or switching equipment" and "providers of telecommunications support services" (as defined in the statute) to cooperate with telecommunications carriers to make available, on reasonable terms and prices, features or modifications necessary to enable the carriers to comply with assistance capability requirements. 47 U.S.C. § 1005(b).

CALEA provides a compliance "safe harbor" to carriers that comply with technical requirements or standards adopted by telecommunications industry associations or standard-setting organizations or by the FCC. 47 U.S.C. § 1006.

C. Policies and Guidelines for Counterterrorism Operations

1. The Attorney General's Guidelines for Domestic FBI Operations

The FBI is also governed by Department of Justice and internal guidelines and policies. The Attorney General's Guidelines for Domestic FBI Operations (AG Guidelines) were issued on September 29, 2008, pursuant to 28 U.S.C. §§ 509, 509A, 510, 533, 534 and Executive Order 12333. Although not specific to counterterrorism, the AG Guidelines are the culmination of the evolution of the FBI and its policies for domestic operations since September 11, 2001. During these years, the FBI reorganized and reoriented its programs and missions, increased focus on compliance issues, and implemented major revisions to its operational policies.

The AG Guidelines apply to FBI investigative and intelligence collection activities in the U.S., its territories, and outside the territories of all nations. They govern most FBI investigative activities in foreign nations because those activities generally arise from authorized domestic investigations. Otherwise, FBI activities in foreign nations are governed by non-superseded sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG) (2003) and the Attorney General's Guidelines for Extraterritorial FBI Operations (1993), which have not been updated since their effective dates.

The AG Guidelines set standards for information-gathering activity, affording the FBI flexibility to adapt the information sought and the methods used to the nature of the investigation and the character of the information supporting the need for investigation. The AG Guidelines define two primary levels of investigation: assessments and predicated investigations.

The AG Guidelines maintain the historical respect for the "least intrusive means" and the exercise of First Amendment and other protected rights. As an overarching control, investigators must consider and use the least intrusive feasible method under the circumstances of obtaining information that is relevant to the purpose of the assessment or investigation. AG Guidelines I.C.2. The AG Guidelines also prohibit the collection or maintenance of information on U.S. persons solely for purposes of monitoring the lawful exercise of First Amendment or other rights secured by the Constitution and investigations based solely on race, ethnicity, national origin, or religion. AG Guidelines I.C.3.

The FBI implemented the AG Guidelines through the Domestic Investigations and Operations Guide (DIOG), which became effective on December 16, 2008. A revised guide, DIOG 2.0, became effective on October 15, 2011.

Assessments. To open an assessment, an FBI Agent must identify the purpose of the assessment in writing and that purpose must be within the FBI's mission (i.e., an "authorized purpose"). No particular factual predication is required, but the basis of an assessment cannot be arbitrary or groundless speculation. Any investigative activity must be related to the purpose of the assessment. See DIOG §§ 5.1-5.3. For example, to carry out its counterterrorism responsibilities, the FBI must draw proactively on available sources of information to identify potential terrorist threats and activities. The FBI cannot wait for leads to come in through the actions of others, but must be vigilant in detecting potential threats and activities to the extent permitted by law, with an eye toward early intervention and prevention. The proactive investigative authority conveyed in assessments is designed to discharge these responsibilities.

The AG Guidelines authorize six types of assessments: the prompt and limited checking of leads that individuals or groups (Type 1 and Type 2) are or may be engaged in criminal behavior or pose a national security threat; the collection of information necessary to the evaluation of threats and vulnerabilities (Type 3) and to facilitate intelligence analysis and gathering (Type 4); information gathering for the limited purpose of identifying, vetting, recruiting, validating, and maintaining the cover or credibility of human sources (Type 5); and the collection of foreign intelligence in response to a national intelligence requirement (Type 6).

AG Guidelines II.A.3. Supervisory approval is required to open all but Type 1 and Type 2 assessments.[3/]

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly-available information, checking government records, and requesting information from members of the public. More intrusive techniques such as electronic surveillance, undercover operations, NSLs, pen registers, and trap-and-trace devices may not be used in assessments. DIOG 2.0 §§ 5.09, 5.10.

Predicated Investigations. Predicated investigations can be based on allegations, reports, facts, or circumstances that indicate possible criminal or national security-threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements. The AG Guidelines require supervisory approval to initiate predicated investigations. AG Guidelines II.B.2.

Predicated investigations that concern federal crimes or threats to the national security are divided into preliminary investigations and full investigations. The FBI may initiate preliminary investigations based on any allegation or information indicative of possible criminal or national security-threatening activity. More substantial predication is required for full investigations. Time limits, which may be extended, are set for the completion of preliminary investigations. Full investigations may be pursued without preset limits on their duration.

Information Sharing / Intelligence Information Reports. The AG Guidelines also govern information sharing. The FBI is responsible for providing "information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing." AG Guidelines VI.D. The FBI must disseminate information in a manner that protects the privacy, civil liberties, and other legal rights of U.S. persons consistent with the Privacy Act of 1974 and other statutes, executive orders, and Presidential directives. Id. at VI.B. The dissemination of information acquired under FISA is subject to minimization procedures and other statutory requirements.

The AG Guidelines authorize the FBI to conduct research, analyze information, and prepare reports and intelligence assessments concerning matters relevant to authorized FBI activities, including terrorism and other threats to the national security. AG Guidelines VI.B. Under this authority, the FBI issues Intelligence Information Reports (IIRs) to share raw intelligence within the FBI and with other members of the U.S. Intelligence Community. "Raw intelligence" refers to unevaluated intelligence information, generally from a single source, which has not been fully evaluated, interpreted, or analyzed. The FBI produced 25,012 IIRs in 2010. *FBI Information Sharing Report*, 21-22 (2010).

[3/] The original DIOG, like the AG Guidelines, authorized six types of assessments. Because Type 1 and Type 2 assessments are essentially identical, varying only in whether they involve an individual or group, DIOG 2.0 combines them and refers to them collectively as "Type 1 & 2 assessments."

To protect privacy and other legal rights of U.S. persons, the DIOG directs that intelligence reports and assessments not contain U.S. person information if the intelligence can be conveyed without including identifying information. DIOG § 15.7.B. Threats can be reported via IIR only if the information is sufficiently detailed and reliable to serve as a basis for preventive action.

Oversight. The AG Guidelines also establish oversight mechanisms for FBI national security investigations. Oversight is accomplished through (1) a dedicated oversight section within DOJ's National Security Division; (2) a dedicated compliance office within the FBI; (3) on-site audits conducted by the FBI's Inspection Division; (4) notices and reports internally and to DOJ; (5) FISC filings; and (6) reports to the President's Intelligence Oversight Board. For example, the AG Guidelines require notifications and reports by the FBI to the National Security Division about the initiation of national security investigations and foreign intelligence collection activities in certain contexts. AG Guidelines, Introduction, VI.D. The AG Guidelines also authorize the Assistant Attorney General for National Security to request additional reports and information about those activities. Id.

All FBI employees are responsible for ensuring that their activities comply with the AG Guidelines, federal statutes, executive orders, and the Constitution. Several offices, including the DOJ Office of Privacy and Civil Liberties, the FBI Privacy and Civil Liberties Unit, the FBI Inspection Division, the FBI Office of General Counsel, and the FBI Office of Integrity and Compliance, are responsible for ensuring that FBI employees fulfill the responsibility to undertake activities authorized by the AG Guidelines in a lawful, appropriate, and ethical manner. A significant component of DOJ National Security Division oversight comes in the form of National Security Reviews, the in-depth reviews of national security investigations that the National Security Division and the FBI Office of General Counsel commenced in 2007. Each FBI Field Office undergoes a National Security Review every three to four years, but reviews may occur more frequently depending on the office's history of compliance.

In 2007, the FBI established the Office of Integrity and Compliance (OIC), modeled after private sector compliance programs, to ensure that national security investigations and other FBI activities are conducted in compliance with the FBI's governing authorities. OIC reports to the Director and focuses the attention of executive management on FBI operations and business processes that pose compliance risks. Through OIC, rather than reacting to problems after they occur, the FBI seeks proactively to identify legal risks and to develop policy and training to mitigate those risks.[4/]

[4/] We believe that OIC can and should play a significant role in proactively ensuring the FBI's compliance with its governing authorities. In Part Five, we recommend that OIC analyze and identify compliance risks associated with investigative techniques that implicate potential risks to civil liberties and privacy interests – and, upon identifying risks, request that the Inspection Division conduct an audit. We understand that OIC is currently conducting a review of reported instances of "substantial non-compliance" with the DIOG, which the Inspection Division will follow with a general audit of DIOG compliance. We believe it is critical that the FBI and, if necessary, Congress make available sufficient personnel and funds to ensure that compliance is achieved.

2. The FBI's Domestic Investigations and Operations Guide

The Domestic Investigations and Operations Guide (DIOG) implements the AG Guidelines. It is a comprehensive, 270-page collection of procedures, standards, approval levels, and explanations designed to update and consolidate policies, procedures, and guidance, and to ensure Special Agent and Intelligence Analyst activities conform to the AG Guidelines. A majority of its text is unclassified and available to the public on the FBI's website. The DIOG's purpose is to standardize policies, procedures, and guidance so that FBI criminal, national security, and foreign intelligence investigative activities are consistent and uniform when possible (for example, by adopting identical approval, notification, and reporting requirements). Many policies had appeared in the Manual of Investigative Operations and Guidelines (MIOG) and memoranda to the field, and had not been re-examined or updated in years.

The DIOG is more restrictive than the AG Guidelines, as well as applicable statutory and constitutional law, in terms of what investigative activities FBI personnel can use and how they can use them. Thus, the DIOG establishes greater overall protections for privacy and civil liberties than the law and DOJ policy require.

In accord with the AG Guidelines, the DIOG prohibits the opening of an assessment based on "arbitrary or groundless speculation"; solely on the exercise of First Amendment rights; or solely on the race, ethnicity, national origin, or religious practice of any person or group, or on a combination of only those factors. DIOG §§ 5.1 and 5.3. The DIOG also stresses the importance of oversight and self-regulation to ensure that all investigative and intelligence collection activities are conducted within Constitutional and statutory parameters.

The FBI also issues Policy Guides to provide program-specific guidance to Agents and Analysts on specific types of investigative activity. The FBI is reviewing and revising its Policy Guides to ensure that they conform to the AG Guidelines. The FBI finalized its revised Policy Guide on Counterterrorism Investigations early in 2012.

When the AG Guidelines and DIOG were adopted, the FBI launched a comprehensive training effort. The primary objective of training was to ensure that FBI personnel understood and could apply new concepts and authorities. Another objective was to reinforce existing guidelines and procedures. The FBI recognized that the introduction of the AG Guidelines and DIOG presented an opportunity to ensure that Agents and Analysts conducted their activities in a consistent and compliant manner, regardless of their location or program of assignment, and to standardize processes that had become inconsistent across Field Offices. To this end, the FBI required more than 20,000 personnel to attend 16.5 hours of live training and to take and pass a test on the DIOG. The FBI implemented a "train-the-trainer" program that deployed more than 100 Headquarters-trained instructors to its 56 Field Offices and Headquarters. These Headquarters-trained personnel then trained additional trainers in their divisions.

An FBI Inspection Division audit of assessments indicates that the training was effective. The Inspection Division audited all 3,426 Type 3 through Type 6 assessments conducted in 2009. Of the 218 errors identified, 176 (80%) occurred prior to DIOG training. [5/]

3. Domestic Investigations and Operations Guide 2.0

When the AG Guidelines and DIOG came into force in 2008, the FBI advised Congress that it planned an extensive re-evaluation of the DIOG, including a review of the adequacy of its protections of civil rights and liberties and privacy. That re-evaluation took approximately 18 months. The FBI considered the need for each proposed revision to the DIOG, the potential risks to civil liberties and privacy rights, and the controls in place.

The FBI informed DOJ of all substantive issues and proposed revisions. Upon completing the re-evaluation, the FBI briefed its Congressional oversight committees and advocacy groups, and adopted certain suggestions received[, including advocacy community suggestions involving the FBI's Undisclosed Participation Policy (UDP).]

The FBI's re-evaluation led to strengthening the protection of civil liberties and privacy rights in some contexts. For example, DIOG 2.0 requires Type 1 & 2 assessments to be based on tips or leads. Id. at § 5.6.3.1. It tightens the approval requirement for [UDP and certain other FBI investigative techniques.]

5/ In 2010, OIG documented DIOG examination abuses and cheating by 22 FBI Agents, including supervisory personnel. OIG Oversight & Review Div., U.S. Dept. of Justice, *Investigation of Allegations of Cheating on the FBI's Domestic Investigations and Operations Guide (DIOG) Exam* (Sept. 2010). Although OIG identified reasons for this conduct, the Inspector General concluded that those reasons did not excuse the conduct. The FBI referred the 22 employees to its Inspection Division. Charges will ultimately be forwarded to the Office of Professional Responsibility for adjudication. The FBI is following established policies and processes to identify any other employees who may have engaged in inappropriate conduct. The FBI has developed a new training module for DIOG 2.0.

The FBI issued DIOG 2.0, effective October 15, 2011. An unclassified version of DIOG 2.0 is available on the FBI's public website.[6/]

Unless otherwise indicated, this Report cites to the original DIOG because that version was in effect at the time of the matters under review.

4. Agreements with Other Departments and Agencies

The FBI's ability to share information with other government departments and agencies is governed not only by its statutory authority, but also by a myriad of agreements. For example, at the time of the Fort Hood shootings, there were more than 100 agreements and Memoranda of Understanding (MOU) between the FBI and the Department of Defense (DoD) that included provisions on information sharing.

At the time of the events under review, a 1979 *Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation* principally governed coordination of FBI and DoD counterintelligence activities. That agreement was amended in 1996 to provide that the FBI advise DoD about counterintelligence investigative interest in persons associated with DoD.

Another MOU governs the participation of DoD personnel in Joint Terrorism Task Forces (JTTFs). That MOU addresses the sharing of information related to counterterrorism investigations with persons who are not JTTF members. DoD participants in JTTFs cannot discuss JTTF investigations or any information gathered during those investigations with any DoD personnel outside the JTTF without an FBI supervisor's approval. However, the MOU directs the FBI to facilitate sharing relevant information with appropriate DoD officials as expeditiously as possible given the constraints of a particular investigation and any law or procedure affecting release of the information.

There are legal restrictions on sharing information. For example, there are restrictions on the dissemination of grand jury information and information that would reveal sources and methods. [redacted] FISA limits what FISA-derived information can be shared, and FISA-required minimization procedures limit how that information can be shared. As noted in Section B.1 above, FISA allows FISA-derived information about non-consenting U.S. persons to be disseminated only if it reasonably appears to be foreign intelligence, necessary to understand foreign intelligence or assess its importance, or evidence of criminal activity.

6/ DIOG 2.0 also authorizes emergency departures from the DIOG without prior approval (if sought within 24 hours of the departure),§ 2.7.3.; allows queries of commercial databases and state, local, and tribal law enforcement records before initiating an assessment (which can weed out unfounded complaints without resort to more intrusive methods), Id. at § 5.1.1; [redacted] and clarifies the definitions of electronic and physical surveillance. Id. at § 18.5.8.1.

Chapter 4

The FBI Information Technology and Document Review Infrastructure

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. In conventional warfare, our soldiers use shoulder arms and handguns. In combating terror, those weapons have a place, but the FBI's crucial weapon is information. Our investigation revealed that the FBI's information technology and information review protocols were then, and are now, less than adequate for fulfilling the FBI's role as the premier U.S. intelligence and law enforcement agency combating domestic terror.

A. The Standard Workstation

At the time of the events at issue – and today – Agents, Analysts, and Task Force Officers (TFOs) in San Diego, Washington, and other JTTFs used desktop computers with commercial off-the-shelf word processing, spreadsheet, and other functionalities common to contemporary business enterprises (for example, Microsoft® Office, Corel® WordPerfect). These computers are linked to classified FBI networks to allow for secure email communications and shared workspace; access to specialized tools ranging from Delta (for management of confidential sources) to FISAMS (an impressive web-based tool for preparing, transmitting, seeking approval for, and tracking FISA requests); and access to FBI and certain other government databases – including, when trained and authorized, classified databases that are central to the workflow of Agents, Analysts, and TFOs working on counterintelligence and counterterrorism squads.

This multi-faceted workstation confronted users in 2008 and 2009 with a non-integrated, sometimes dated, and at times clumsy toolset rather than an integrated, user-friendly suite of tools. Users had to log in to the desktop computer, then log in separately, as necessary, to a series of discrete tools and databases, each with its own password and its own search tool (and thus, its own search methodology). Prior to the Fort Hood shootings, training on these tools and databases was limited or non-existent. Agents, Analysts, and TFOs typically learned the basics of each tool and database on the job rather than through formal instruction.

B. The Standard Toolset

1. Data Warehouse System/Electronic Surveillance Data Management System

(a) Overview

The primary database relevant to our investigation is the Data Warehouse System-Electronic Surveillance Data Management System (DWS-EDMS). Designed and developed by the FBI's Special Technologies and Applications Section (STAS), DWS is an access-controlled, text-oriented database of [information acquired through the FBI's exercise of its criminal and counterterrorism authorities and techniques (see Chapter 3).] [redacted].

As of July 2011, the holdings of DWS-EDMS exceeded [redacted] of data. [redacted] Its holdings increase, on average, by [redacted] new files – approximately [redacted] of data – each week.

STAS designed DWS in 2001 as a transactional database to record [communications intercepts] [redacted]. In the intervening years, DWS became the depository of [redacted] information obtained [through exercise of the FBI's governing authorities and techniques] [redacted]. Although not designed as a warehouse database, it has become one. Thus, although it is a capable, if overburdened, tool for the conventional review of [redacted] [information], DWS was not originally designed for the review and management of large strategic intelligence collections [redacted]. It also lacks the modern hardware infrastructure needed to fulfill and preserve its functionality.

DWS was the system in place in December 2008 [when Hasan sent his first message to Aulaqi] [redacted]. STAS upgraded the system to DWS-EDMS in February 2009. The EDMS functionality assists Language Analysts [redacted]. STAS again upgraded the system in May 2009, by implementing a new Graphic User Interface (GUI). The prior GUI remained operational under the name DWS-EDMS Classic. Unless a distinction is appropriate, this Report discusses all three systems as DWS-EDMS.

In FBI parlance, email accounts, telephone numbers, and other targets of electronic surveillance are known as "facilities." As of July 2011, DWS-EDMS held [redacted] [communications] from [redacted] facilities in [redacted] cases. [redacted] [Communications and other information stored in DWS-EDMS] are called "products." [redacted]

[redacted]

FBI systems process [redacted] and load [acquired information] [redacted] into DWS-EDMS, which indexes each file's text and metadata for searching. [redacted]

(b) **The Interface**

To work in DWS-EDMS, the user logs in [redacted] [and is taken] to a Home page that contains announcements and advisories to assist users, including a list of the user's active cases with [redacted] [information stored in DWS-EDMS]. [redacted]

The primary review screen [redacted] is similar to a Microsoft® Outlook Mailbox. The top of the screen has a series of drop-down menus. Beneath that, on the left, is an identifier of the selected case and facility. On the right is a Filters workspace that allows the user to select filtering criteria to assist in reviewing the [redacted] [information]. Beneath that is a column [displaying each product] [redacted] much like an email Inbox.

The user can select a product for review by double-clicking it, which opens the product on the right-hand side of the screen. A workspace above the product allows the user to add notes and translations, and tag any foreign languages used. A workspace column to the left of the product provides identifying information about the product; allows filtering of products by type; and provides checkboxes for [redacted] [identifying] the product for [, among other things,] [redacted] Workflow, Translation, and Attorney-Client Privilege.

(c) **Search Capabilities**

Because of its original design as a transactional database, DWS-EDMS has limited search and information management capabilities to support the review [redacted] [redacted] [of acquired] products. Those tools were not designed for and do not provide effective assistance for the review and management of [massive collections of information, like the collection in the the Aulaqi investigation.] [redacted]

DWS-EDMS search capabilities are limited. The primary search modes are by [redacted]. Keyword searches can use wildcards (for example, bomb* to return variants such as bombs, bombers, bombed,

bombing) and Boolean operators (for example, Nidal AND Hasan to return all products using those two words, or Nidal OR Hasan to return all documents using one of those two words). These searches are literal and return only documents containing the specified [redacted]. The search engine lacks [redacted] functionalities [redacted] (see Part Two, Chapter 11 and Part Five: Recommendations). More important, search results may be affected by the user's search technique. As discussed in Chapters 7 and 11, a "full text" search of DWS-EDMS for NidalHasan@aol.com as of November 5, 2009, returns only half of the messages at issue, while an email "participant" search returns all of them.

(d) Information Management Capabilities

Until February 2009, DWS had no tools for [tracking and correlating certain email data] [redacted]. A new message could be linked with an earlier message only through memory, notes, or by actively searching the system.

In February 2009, the DWS-EDMS upgrade gave users the ability to customize their Home screen by specifying [certain] Favorites, [including] [redacted] Favorite Cases, Favorite Products, and Favorite Tools. [redacted] Favorite Products allowed users to access specified products from their Home screen. Users could also activate [redacted] [notifications] for a specified facility [redacted]. Users could also copy messages to a folder on the main review screen and share those messages with others with authorized access.

Prior to the Fort Hood shootings, reviewers had no direct [or automated] means of linking [certain email data with other email data] [redacted] To locate and review [redacted] [communications] between two persons, users had to search the system [redacted].

(e) Training

To obtain DWS-EDMS access, an Agent, Analyst, or TFO must first complete three training courses in the FBI's Virtual Academy: (1) Foreign Intelligence Surveillance Act (FISA) Section 702 Retention; (2) 2008 FISA Standard Minimization Procedures (SMP) Overview; and (3) 2008 FISA Standard Minimization Procedures (SMP) – Policy Implementation Guidelines. The Agent, Analyst, or TFO must also review the SMP Implementation Policy (0137D); Access Policy for EDMS, DWS, DaLAS and any Successor Systems (0285D); and Rules of Behavior.

None of these courses provides instruction on how to use the DWS-EDMS search tool or other functionalities.

Many Agents and Analysts – and most TFOs – did not receive training on, or access to, DWS-EDMS and other FBI databases until after the FBI's internal investigation of the Fort Hood shootings. Even for Agents and Analysts with access before the Fort Hood shootings, there was no formal training program for DWS-EDMS; instead, most "training" occurred on the job.

(f) Disaster Recovery Capability

Although DWS-EDMS is one of the FBI's primary workhorse systems, it has no "live" or "failover" disaster recovery backup. [redacted] System shutdown or database corruption would require [redacted]

2. Other Databases

DWS-EDMS cannot be viewed in a vacuum. Agents, Analysts, and TFOs also rely on a large number of other databases. Some databases are unique to the FBI. Others are unique to a given TFO's home department or agency, and can be accessed only by TFOs from that department or agency. Others belong to other government departments and agencies that have agreed to allow access through FBI systems.

The FBI's primary databases include:

Automated Case Support (ACS), which consists, in turn, of three independent structured data applications:

- The **Universal Index (UNI)**, a database of identifying information derived from FBI investigations (including subjects, witnesses, complainants, addresses, telephone numbers, and email addresses). UNI, which is accessed using a DOS-based tool that dates to the 1990s, contains more than [redacted] records.
- The **Electronic Case File (ECF)**, which provides for electronic filing and cataloguing of case-specific documents (serials) and information. ECF is the source of the FBI's standardized Electronic Communication (EC), which replaced letters, faxes, and memoranda for internal communications. ECF contains more than [redacted] records.
- **Investigative Case Management (ICM)**, which provides for the entry and management of case information, including leads and ticklers.

Sentinel. Although central to the everyday tasks of Agents, Analysts, and TFOs – and the most frequently used FBI system – ACS is also the FBI's most outdated system. It is being phased out in favor of an impressive Web-based successor, Sentinel.

Investigative Data Warehouse (IDW). IDW ranks second to ACS in use for investigation and analysis. IDW holds more than [redacted] investigative and intelligence records from the FBI (including limited data collections from ACS-UNI, ACS-ECF, and ACS-ICM), other government agencies, and outside entities – at this writing, more than [redacted] databases, primarily non-FBI in origin. IDW is more than [redacted] in size.

IDW has special tools to assist in refined searches of popular data collections [redacted]. Its primary search tool [redacted] differs significantly from the limited [redacted] DWS-EDMS search tool in place at the time of the events at issue.[7/]

Data Loading and Analysis System (DaLAS). This web-based system holds data acquired by FBI Field Offices or the United States Intelligence Community (USIC) as digital evidence (for example, CD-ROMs, DVDs, hard drives, cellular phones, and raw network feeds) and scans of documents seized in counterintelligence and counterterrorism investigations. DaLAS automates data uploading, processing, and classification of these media for analysis. DaLAS then provides a searchable, central repository of that data, enabling investigators and analysts at diverse locations to collaborate on projects or cases using Bureau-approved platforms.

As of May 2011, DaLAS hosted more than [redacted] files totaling [redacted] in size. [redacted]

Telephone Applications. This investigative database consists of telephone transactional records ("what number called what number") collected using authorized investigative methods.

Clearwater. This non-investigative, intelligence database provides authorized users with access to telephone numbers, email addresses, and other electronic communications transactional records and sources derived from FBI and other USIC members.

7/ [redacted]

Guardian and **eGuardian.** Guardian is the FBI's terrorism threat tracking and management system. The FBI's written Guardian policy requires all personnel to enter all new terrorism-related threats, events, and suspicious activities – including new Type 1 & 2 assessments – into the system as a Guardian "incident." Guardian thus serves as the primary database for setting leads to other Field Offices and JTTFs to open new terrorism-related assessments or investigations.

eGuardian is a secure enhancement of Guardian that shares unclassified information about terrorism-related threats, events, and suspicious activities with approved state, local, tribal, and other federal law enforcement agencies, including state fusion centers and regional intelligence centers. These agencies, in turn, can use eGuardian to report terrorism-related threats, events, and suspicious activities to the FBI and other participating agencies. The FBI reviews these reports to determine whether to create a Guardian incident and pursue an assessment or investigation.

Although Guardian is accessible to all authorized Agents, Analysts, and TFOs, larger Field Offices and JTTFs have discrete Guardian squads to assess and resolve Guardian incidents. At smaller locations, individual Agents and TFOs are assigned ongoing responsibility for Guardian incidents.

C. The Lack of Data Aggregation

The FBI possesses more than [redacted] investigative and intelligence databases. Agents and Analysts regularly consult more than [redacted] of those databases in the performance of their duties. At the time of the Fort Hood shootings, however, with a few exceptions (notably IDW), users accessed each database using a discrete interface, a discrete password, and a discrete search engine. DWS-EDMS users could not conduct a simultaneous search of that system and the contents of any other FBI or other government agency database. Although the absence of this functionality did not directly affect the FBI's handling of the Hasan information, 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.

Chapter 5

The FBI's Investigation of Anwar Al-Aulaqi

The United States confronts a wide range of international and domestic terror threats. As of September 2011, the FBI was pursuing nearly [redacted] international terrorism investigations.

The FBI prioritizes counterterrorism cases in [redacted] tiers. [redacted] [The redacted portion describes sensitive FBI investigative techniques.]

As of September 2011, there were more than [redacted] Tier [redacted] and [redacted] Tier [redacted] international terrorism investigations in progress.

The FBI acquired its information on Nidal Hasan during the course of its investigation of Anwar Nasser al-Aulaqi (sometimes spelled "Awlaki"). At the time, the Aulaqi case was [redacted] a Tier [redacted] investigation [of a suspected radicalizer/recruiter].

A. Background

Aulaqi was born on April 21, 1971, in Las Cruces, New Mexico. He attended primary and secondary school in Yemen from 1979 to 1990. He received a Bachelor of Science in Civil Engineering from Colorado State University in 1994. He then moved to San Diego, California, where he served as an imam at the Al-Ribat Mosque from December 1995 until mid-2000.

[redacted] [During his time in San Diego, the] San Diego JTTF opened a preliminary investigation of Aulaqi [redacted] [The redacted portion describes the predicate for this investigation.]

At the beginning of 2001, Aulaqi moved to Falls Church, Virginia. He was an imam at the Dar al-Hijrah mosque in Falls Church from January 2001 until April 2002. [redacted]

[redacted] [The redacted portion describes certain information the FBI learned about Aulaqi during this time frame.] WFO opened a full investigation. [redacted]

In March 2002, Aulaqi moved to England, where he reportedly lectured youth groups on jihad. WFO closed its investigation of Aulaqi in May 2003 for lack of evidence of a pattern of activity suggesting international terrorism. In 2004, Aulaqi moved to Yemen.

In January 2006, the WFO reopened its investigation based on [redacted]

In April 2006, the FBI transferred the Aulaqi investigation back to the San Diego JTTF. [redacted]

Later in 2006, Yemeni authorities arrested and imprisoned Aulaqi on kidnapping charges. [redacted] Aulaqi was released from prison in December 2007.

Aulaqi is a prime example of a radicalization leader. He established and sustained an international reputation as a prolix, charismatic imam who provided Islamic guidance in English through sermons, lectures, publications, recordings, and a website. For many years, he blurred his anti-Western rhetoric with mundane religious observations and advice. Communications with Aulaqi through his website could involve simple questions about how Western lifestyles comported with or could be reconciled with the teachings of the Quran (as interpreted, of course, by Aulaqi). But his rhetoric increasingly included public statements – and exhortations of violence – against the U.S. Lectures like "Constants on the Path of Jihad" and "44 Ways to Support Jihad," which circulated on the Internet as audio files, provided the stimulus and opportunity necessary for radicalization.

During the past two years, Aulaqi or his rhetoric may have inspired or played a role in encouraging at least four known "homegrown" U.S. radicals who took or attempted violent acts or training: Hasan, Michael Finton, Faisal Shahzad, and Zachary Chesser. For each of them, the connection with Aulaqi was virtual (although Hasan claimed to have met Aulaqi briefly in the early 2000s at the Dar al-Hijrah mosque in Falls Church, Virginia.) The FBI is not aware of any evidence that Aulaqi instructed any of these individuals to engage in violent acts.

B. The [DWS-EDMS Collection] [redacted]

In 2008, the San Diego JTTF consisted of five squads, each led by a Supervisory Special Agent (SSA): three International Terrorism squads, a Domestic Terrorism squad, and a Threat squad. In addition to the five SSAs, the JTTF included 25 FBI Special Agents, five FBI Intelligence Analysts, and 36 full-time Task Force Officers (TFOs) from 20 different federal, state, and local agencies.

[The redacted portion describes sensitive investigative steps taken by the San Diego JTTF.]

San Diego had assigned the Aulaqi investigation to Squad CT-3 . FBI Special Agent (SA) SD-Agent and FBI Intelligence Analyst (IA) SD-Analyst, both members of CT-3, were assigned responsibility for reviewing [information] using DWS. Their Supervising Special Agent was SD-SSA.

By 2008, Aulaqi had established an international reputation as a popular English-speaking Islamic cleric with a prolific output of writings, sermons, and audio recordings as well as a website devoted to his teachings and his anti-Western views. At the same time, his works from the early 2000s, which provided a contemporary interpretation of Islamic matters for an English-speaking audience, were popular among a wider, more mainstream audience. Through his website, Aulaqi would answer mundane questions about Islam for Western followers on topics such as divorce and fasting during Ramadan. He appeared to understand legal limitations. He was not known directly to have instructed anyone contacting him through his website to engage in violent action.

SD-Agent and SD-Analyst believed that Aulaqi had [ambitions beyond radicalization] Their primary purpose was to gather and, when appropriate, disseminate intelligence within the U.S. Intelligence Community about Aulaqi . Between March 2008 and the Fort Hood shootings in November 2009, the [Aulaqi investigation] produced approximately leads and investigations, as well as some Information Intelligence Reports (IIRs). [The redacted portion describes FBI investigative strategy.]

Visitors to [Aulaqi's web]site could select a "Contact the Sheikh" link, which opened a web page that allowed them to type a message to Aulaqi and enter their email address. The message was not posted on the site or otherwise available for public viewing. Instead, the website automatically forwarded the message by email to al_aulaqi@yahoo.com.

The [DWS-EDMS collection] presented, in SD-Analyst's words, a "crushing volume" of information, confronting SD-Agent and SD-Analyst with [thousands of electronic documents] for review. SD-Agent spent

approximately three hours each day reviewing [this information] . SD-Analyst spent about 40% of his time on the investigation.

On a typical morning in late 2008, SD-Agent and SD-Analyst would log in to DWS to review [information] . SD-Analyst usually read [certain information] while SD-Agent [read other information] . It was not unusual, however, for both men to [read everything]

[T]hrough December 17, 2008, the date of Hasan's first message to Aulaqi, [SD-Agent and SD-Analyst reviewed] 12,799 [electronic documents – on average,] 1,420 per month, or 65 to 70 per work day.

Between December 17, 2008, the date of Hasan's first message to Aulaqi, and June 16, 2009, the date of his last message SD-Agent and/or SD-Analyst reviewed 7,143 [electronic documents] [or, on average,] 65 to 70 per work day. [T]he workload could vary dramatically. As the following chart reveals, [during portions of this timeframe, SD-Agent and SD-Analyst had to review, on average, as many as 132 electronic documents per work day.]

[The redacted portion involves FBI investigative techniques and classified details about the investigation workload.]

C. The Workflow

1. [Identification] Requirements

[The FBI's governing authorities] required SD-Agent and SD-Analyst to make [multiple] decisions about each DWS-EDMS [electronic document, including] Attorney-Client Privilege.

SD-Agent had ultimate authority for the [identifications]. If SD-Analyst had questions SD-Agent would make the final decision.

[redacted]

[redacted]

[redacted]

Workflow. Reviewers use Workflow [redacted] [identifications] to assist in managing and tracking products. [redacted]

[redacted]

Translation. These [identifications] [redacted] enable users to identify products that need translation.

[redacted]

Attorney-Client Privilege. These [identifications] [redacted] enable users to identify products that may be subject to attorney-client privilege.

[The redacted portions describe classified and sensitive FBI identification requirements.]

D. Human Factors

Research shows that trained information reviewers faced with binary decisions like those made by [SD-Agent and SD-Analyst] [redacted] – relevant/irrelevant, responsive/non-responsive, pertinent/non-pertinent – identify only about 75% of the relevant documents and, indeed, agree with each other's decisions only about 75% of the time.

The Text Retrieval Conference (TREC), a project co-sponsored by the National Institute for Standards and Technology and the U.S. Department of Defense, conducts comparative research on text retrieval technologies. In 2008, the TREC Legal Track assembled volunteer research teams consisting primarily of second- and third-year law students, augmented by recent law school graduates, experienced paralegals, and litigation specialists. Each reviewer assessed the relevance or non-relevance of 500 documents, at an average rate of approximately 21.5 documents per hour. In 2006 and 2007, other reviewers had judged the relevance or non-relevance of samples of the same documents. The reviewers agreed on relevance decisions only 71.3% of the time. See Oard, Hedin, et al., 2009; Tomlinson, Oard, et al., 2008; Baron, Lewis & Oard, 2007.

Other studies have found comparable levels of agreement. The Electronic Discovery Institute (EDI), a non-profit research institution that studies human and technology-assisted document review, assessed a four-month review of 1.6 million documents by attorneys for Verizon. Two new teams of attorneys conducted independent reviews of a sample set of 5,000 documents. The teams agreed on relevance decisions only 70% to 76% of the time. See Roitblat, Kershaw & Oot, *Document Categorization in Legal Electronic Discovery: Computer Classification vs. Manual Review*, J. AM. SOC. INFO. SCIENCE & TECH. 61(1):70-80, January 2010; see also Barnett, et al., *Machine Learning Classification for Document Review*, XEROX RESEARCH CENTER EUROPE/XEROX LITIGATION SERVICES, 2009.

Although differences in the background and experience of reviewers, as well as extrinsic and random factors (for example, inattention, distraction, fatigue, or illness) can produce variations in accurate decision-making about the relevance [redacted] of information, other primary factors include the nature of language; reviewer workload; the size and pace of information collection; the complexity of the information under

review; the [redacted] [identification] requirements; the available information review and management tools; the available computer technology and infrastructure; training; and the availability of managed quality control.

E. The Language Barrier

The inherent ambiguity of language and the presence of jargon, idiom, foreign languages, and code challenge even the most capable reviewers and search technologies. A classic study measured the accuracy of attorneys and other experienced review professionals in conducting computer-assisted searches of 40,000 documents in order to determine their relevance or non-relevance to a train accident. See Blair & Maron, *An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System*, 28 COMM. ACM 289 (1985). Although the reviewers estimated that their search methodology had identified more than 75% of the relevant documents, they located only about 20%.

The disparity resulted from the myriad of ways in which the documents used the English language; for example, describing the accident as an "incident," "disaster," "event," "situation," "problem," and "difficulty." The study concluded: "It is impossibly difficult for users to predict the exact words, word combinations, and phrases that are used by all (or most) relevant documents and only (or primarily) by those documents." Blair & Maron, at 295.

The potential involvement of foreign languages only exacerbates the challenges for FBI reviewers. Because of Aulaqi's U.S. origin and celebrity as an English-speaking imam, the [redacted] communications at issue are almost entirely in English, with occasional Arabic salutations, references, and quotations from the Quran. As a result, these communications did not confront reviewers with an ongoing need for translation services, which can delay access to products and complicate searches.[8/]

F. The "Trip Wire"

The Aulaqi [investigation] [redacted] also served as an occasional "trip wire" for identifying [redacted] persons of potential interest [redacted]. When SD-Agent or SD-Analyst identified such a person, their typical first step was to search DWS-EDMS and other FBI databases for additional information [redacted]. If the [redacted] [person] was a U.S. Person or located in the U.S., SD-Agent might set a lead to the relevant FBI Field Office. If the information was believed valuable to the greater intelligence community and met one of the FBI's intelligence-collection requirements, SD-Analyst would disseminate it outside the FBI in an IIR. Indeed, section 1.7 of the FBI Intelligence Policy Manual requires dissemination of intelligence that has the potential to protect the U.S. against threats to national security or improve the effectiveness of law enforcement. See FBI Intelligence Information Report Handbook § 4.1.2; *Privacy Impact Statement for the FBI*, FBI Intelligence Information Report Dissemination Systems (FIDS) § 1.1 (July 2, 2010).

8/ We heard anecdotal evidence of a lack of sufficient human translation resources. [redacted] Although developers have achieved remarkable advances in auto-translation, computers are not yet adequate substitutes for translators.

Chapter 6

The FBI's Assessment of Nidal Malik Hasan

A. San Diego: December 17, 2008 – January 7, 2009

On December 17, 2008, Nidal Hasan tripped the wire. He visited www.anwar-alawlaki.com. Using the website's "Contact the Sheikh" tool, he wrote a message to Aulaqi that included a personal email address, NidalHasan@aol.com. The website transferred that message by email to al_aulaqi@yahoo.com. [redacted] [The FBI acquired the] email and uploaded it to DWS.

[redacted] SD-Analyst reviewed Hasan's message to Aulaqi, which read:

> Nidal Hasan wrote:
> Assalum Alaikum Wa Rhahmutallahi Wa Barakatu,
>
> There are many soldiers in the us armed forces that have converted to Islam while in the service. There are also many Muslims who join the armed forces for a myriad of different reasons.
> Some appear to have internal conflicts and have even killed or tried to kill other us soldiers in the name of Islam i.e. Hasan Akbar, etc. Others feel that there is no conflict.
> Previous Fatwas seem vague and not very definitive.
> Can you make some general comments about Muslims in the u.s. military.
>
> Would you consider someone like Hasan Akbar or other soldiers that have committed such acts with the goal of helping Muslims/Islam (Lets just assume this for now) fighting Jihad and if they did die would you consider them shaheeds.
>
> I realize that these are difficult questions but you seem to be one of the only ones that has lived in the u.s. has a good understadning of the the Qur'an and Sunna and is not afraid of being direct.
>
> Jazaka'Allah Khair.

This message and most of the messages and emails that followed contain misspellings and other typographical errors. We present all texts in their original form, without corrections.

SD-Analyst brought the message to SD-Agent's attention. SD-Agent [redacted] [identified] the email as a "Product of Interest." He traced the IP address to Reston, Virginia. (An IP address is a unique identifier assigned to a Transmission Control Protocol/Internet Protocol (TCP/IP) host – for example, a computer or mobile phone – when it connects to the Internet or a network. In theory, tracing ("resolving") an IP address should identify the Internet Service

Provider for, and geographic location of, the computer or other device used to send or receive an email or to visit a website.)[9/]

Because the message referenced the U.S. military and its IP address resolved to Northern Virginia, SD-Agent contacted DoD representatives on the San Diego JTTF to help assess the communication. He emailed the message to three Task Force Officers (TFOs): Naval Criminal Investigative Service (NCIS) Special Agent SD-TFO1 and NCIS Intelligence Analyst SD-TFO2, who served on CT-3; and DCIS Special Agent SD-TFO3, who served on another counterterrorism squad. SD-Agent's email included the full text of Hasan's message and noted:

> Here's another e-mail sent to Aulaqi by a guy who appears to be interested in the military. The header information suggests that his name is "Nidal Hasan", but that might not be true. The IP address resolves to Reston, VA. Here's the full text of the message:
>
> ...
>
> Can we check to see if this guy is a military member? Also, I would like your input, from the military standpoint, on whether or not this should be disseminated further. Thanks,

SD-TFO3 joined the San Diego JTTF in 2008. He did not know that DWS-EDMS existed until after the shootings. At that time, he learned that less than half of his squad – including Agents, Analysts, and TFOs – had ever heard of DWS-EDMS. He received training on the system in January 2010. As of the date of our interview in 2011, he had not had an investigative need to request access.

SD-TFO1 joined the San Diego JTTF in 2008. He knew about DWS, but at that time, a common practice was to ask IAs with DWS access to search [redacted] [information from acquired communications]. He received access to DWS-EDMS in December 2009 and received mandatory training in 2010.

SD-TFO2 joined the San Diego JTTF full-time in 2006; she received training on DWS-EDMS in April 2009, but did not have access until December 2009.

SD-TFO3 searched for "Nidal Hasan" in the Defense Employee Interactive Data System (DEIDS) and other DoD databases, without success. On December 19, 2008, he advised SD-Agent that Hasan was not a member of the military.

9/ The FBI uses IP addresses as a guidance tool, not an identifier. IP resolution is an imprecise and often meaningless inquiry. Unrelated persons could be assigned the same IP address at different times during the day on different computers, notably when using public hubs (for example, an Internet café or coffee shop) or if their service provider uses dynamic IP allocation, which assigns IP addresses temporarily and changes them each time a customer logs on. Moreover, knowledge that IP addresses leave a digital footprint has led [redacted] [wrongdoers] (notably child pornographers) to use anonymizers and other techniques or tools to thwart IP address searches.

On January 1, 2009, Hasan sent a second message to Aulaqi through the website. [redacted] SD-Analyst and SD-Agent reviewed that message. Its full text read:

> Nidal Hasan wrote:
>
> Assalum Alaikum Wa-RhamatuAllahi Wa-Barakatu,
>
> Imam, It seems as though Iran is the only government that is not afraid to openly voice its discontent in a straight forward and firm way. I am curious about your opinion in regards to Israeli catalzing unitiy [sic] among all Muslims regardless of specific religious difference. Additionally, is it better for Muslims to say I am just Muslim and not Sunni or shia which seems to divide us.
>
> Jazak-Allah Khair.

SD-Agent [redacted] [identified] this message as "Not a Product of Interest."

On January 7, 2009, SD-TFO2 emailed SD-Agent:

> [SD-Agent],
>
> Though [SD-TFO3]'s research indicates that Nidal is not a military member, I still think this would make a good [Intelligence Information Report]. There might be other information out there that links him to the military in some way. [redacted]
>
> Please let me know if it goes out in an IIR. I'll see if my HQ can eval it.
>
> [SD-TFO3]—did you check to see what other Hasan's are in the military? [redacted] If not, I can have our guy run just the last name.

[The redacted portion involves classified and sensitive FBI investigative information.]

Later that day, after additional checks in DEIDS and other databases, SD-TFO3 located an active duty U.S. Army officer named Nidal Malik Hasan assigned to Walter Reed Army Medical Center in Washington, D.C. He informed SD-Agent of Hasan's probable identity and gave him a print-out of the DEIDS record. The DEIDS record abbreviated "Commissioned Officer" as "Comm Officer " SD-TFO3 misinterpreted the abbreviation to mean "Communications Officer."

SD-Agent searched DWS to determine whether Aulaqi had responded to Hasan's December 17, 2008, message. He had not. However, the search returned Hasan's January 1, 2009, message. SD-Analyst traced its IP address to Washington, D.C. (SD-Agent performed a "participant" search of DWS, rather than a full text search; otherwise, DWS would not have found the second message.)

SD-Agent and SD-Analyst discussed issuing an IIR about Hasan's messages. Given his understanding that Hasan could be a Communications Officer, SD-Agent feared that Hasan might have access to IIRs and thus could learn about the Aulaqi [investigation.] [redacted] SD-Agent decided not to issue an IIR.

SD-Agent prepared, and SD-SSA approved, an Electronic Communication (EC) setting two leads.

A lead is "a request for investigation to assist in bringing a case to a logical conclusion." Manual of Administrative Operations and Procedures (MAOP) § 10.2.9(1). Then-existing FBI policies identified three types of leads: Action Required, Discretionary Action, and Information Only. "Action Required leads are used if the sending office requires the receiving office to take some type of action.... Discretionary Action leads are used if the sending office has some information that may be of importance to the receiving office. These leads may or may not require action by the recipient, and the recipient will decide what, if any, action to take.... Information Only leads are used for information only and when no specific action is required or necessary." MAOP § 10.2.9(1)(a)-(c).

The Manual of Investigative Operations and Guidelines (MIOG), Part II, § 16-1.4(2) also required the originator of a lead to assign "precedence designators" to each addressee. These designators specified the desired speed of response: Immediate, Priority, or Routine. The Manual instructs the originator of a lead to:

> (b) Use the Immediate designator when addressee(s) must take prompt action or have an urgent need for the information....
>
> (c) Use the Priority designator when addressee(s) must have the information or take action within 24 hours....
>
> (d) Use the Routine designator when addressee(s) must have the information in the normal course of business.

SD-Agent had set prior "trip wire" leads to other JTTFs from the Aulaqi [investigation] [redacted]. Each had been a Routine Discretionary Action lead.

San Diego's EC (inadvertently dated January 7, 2008, rather than 2009) set a Routine Discretionary Action lead to the Washington, D.C., Field Office (WFO) because Nidal Malik Hasan appeared to be living or working in its Area of Responsibility. San Diego set the lead "For action deemed appropriate. San Diego requests that WFO notify San Diego if any action is taken based on this information."

The EC provided basic information about Aulaqi and San Diego's investigation, then set forth the complete text of Hasan's two messages and advised that Aulaqi had not responded. The EC described Hasan's possible military status and provided his home address and telephone number. The EC concluded:

> While email contact with Aulaqi does not necessarily indicate participation in terrorist-related matters, Aulaqi's reputation,

> background, and anti-U.S. sentiments are well known [redacted]. Although the content of these messages was not overtly nefarious, this type of contact with Aulaqi would be of concern if the writer is actually the individual identified above.

[The redacted portion involves classified and sensitive FBI investigative information.]

SD-Agent emailed copies of the lead to SD-TFO1, SD-TFO2, and SD-TFO3.

Under written FBI policy, "the recipient will decide what, if any, action to take" on a Discretionary Action lead. MAOP § 10.2.9(1)(a)-(c). SD-Agent expected WFO to take investigative action, including, at the least, contacting DoD and conducting an interview of Hasan, presumably using a pretext. However, San Diego's principal target was Aulaqi, and SD-Agent did not view the Hasan information as important to, or something that would further, the Aulaqi investigation. He did not plan to monitor the lead or follow WFO's actions, if any, in response.

The EC also set an Information Only lead to a Headquarters unit – International Terrorism Operations Section (ITOS) 1, Continental United States (CONUS) 6 – to "read and clear" the EC. ITOS 1 supports, coordinates, and oversees all FBI CONUS-based international terrorism investigations. CONUS 6 is the ITOS 1 unit with regional responsibility for overseeing intelligence collection and investigative efforts by the San Diego JTTF. ITOS1-SSA, ITOS1-Analyst, and ITOS1-Agent received the EC at ITOS 1, CONUS 6. SD-Agent's cover email to these personnel stated:

> This one is for WFO. The individual is likely an Army communications officer stationed at Walter Reed. I would recommend that this not be disseminated as an IIR, since he may have access to message traffic. If this needs to get to the military, WFO might have to do it internally.

Because the available information did not decisively define a terrorism-related threat – and because San Diego set the lead as part of an ongoing investigation – Guardian policy did not require San Diego to create a Guardian incident.

SD-SSA left San Diego in January 2009 to become Assistant Special Agent in Charge (ASAC) [of another FBI office] [redacted]. SD-Agent became the acting Supervisory Special Agent for CT-3 on or about January 19, 2009, and held that position until mid-July 2009. His supervisor in that position was the Counterterrorism ASAC of the San Diego Field Office.

B. Washington, D.C.: January 7, 2009 — February 25, 2009

The Counterterrorism Division in the Washington Field Office includes several FBI-only counterterrorism squads, as well as the Washington, D.C., JTTF (WFO). In 2009, the JTTF at WFO consisted of four squads, each led by an FBI Supervisory Special Agent (SSA): an International Terrorism squad (CT-1), a Guardian squad, a Domestic Terrorism squad, and the

National Capital Response squad. CT-1 consisted of 12 FBI Special Agents, 10 TFOs, one IA, and its SSA, WFO-SSA.

No FBI written policy specifies which office has ultimate responsibility for inter-office leads. In practice, the receiving office owns the lead. That office is responsible for conducting an assessment/investigation in response to the lead and determining what, if any, additional investigative steps are warranted. As a matter of practice, WFO thus owned the Hasan lead and bore ultimate responsibility for its outcome.

SD-Agent set the lead to WFO CT-1 on January 7, 2009. The FBI has no written policy on when the receiving office should assign a lead set by EC. (In comparison, FBI policy requires that supervisors assign Guardian-based assessments within five business days of receipt.)

WFO-SSA did not review and assign San Diego's lead until nearly two months later, on or about February 25, 2009. The delay may have been caused, in part, by WFO's focus on imminent threats relating to the election and inauguration of President Barack Obama.

According to FBI statistics, WFO CT-1 covered [redacted] leads in 2009 – on average, [redacted] leads per squad member.

C. San Diego: January 7, 2009 – February 25, 2009

Between January 7, 2009, and February 25, 2009, [SD-Agent and SD-Analyst reviewed at least 3,000 electronic documents in the Aulaqi investigation.] [redacted] Hasan sent six [messages to Aulaqi] [redacted]. Aulaqi responded to Hasan twice. SD-Agent and SD-Analyst were the only FBI personnel who reviewed these emails. They did not associate these messages with Hasan's initial messages or the lead.

At the time San Diego set the Hasan lead, DWS had no [redacted] [capability for tracking and correlating certain email data. A new message could be linked with an earlier message only through memory, notes, or by actively searching the system]. (see Part Two, Chapter 11).

Because of these shortcomings, Agents, Analysts, and TFOs had to track [and correlate certain email data] [redacted] outside of the system. SD-Agent relied primarily on memory and notes for this purpose. SD-Analyst used an Excel spreadsheet. He did not add Nidal Hasan or NidalHasan@aol.com to his spreadsheet. (Although SD-Analyst also used Favorites to track email addresses of interest, those functionalities were not available until well after San Diego set the Hasan lead.)

On January 16, 2009, Hasan sent his third message to Aulaqi through the website application:

> Nidal Hasan wrote:
> Asalaum Alaikum, Please comment if my flow of logic is correct. JazakAllah Khair,
>
> Is it Permissible to Fire Unguided Rockets into Israel
> There is no question that firing unguided rockets into Israel has the potential of indiscriminately killing civilians. The real question is why Hamas would do such a thing. Can one envision a scenario where it would be acceptable to so. Well, what if Israel was and continues to indiscriminately kill and hurt civilians and commit other atrocities in the Gaza territory to serve their expansionary ambitions. One can then begin to at least understand why the Palestinians would do such a thing. In fact it is probably one of the only things they can do to in an attempt to avenge themselves and repulse the enemy.
>
> Realistically it"s akin to a mosquito attacking a man i.e. it"s uncomfortable and annoying but not a real threat. One may consider the firing of missiles into Israel a transgression in the eye of Allah (SWT) because of its indiscriminate nature. However, it one recalls the verse about the permissibility of transgressing albeit a different scenario I believe it still applies. Verse 2:194 states ""The sacred mont, is for the sacred month, and for the prohibited things, there is the Law of Equality (Qisas). Then whoever transgresses the prohibition against you, you transgress likewise against him. And fear Allah (SWT), and know that Allah (SWT) is with AI-Muttaqun. Other verses that seem to apply include the following.
>
> 1. And those who when an oppressive wrong is inflicted on them(are not cowed but)help and defend themselves. (42:39)
>
> 2. The recompense for an injury is an injury equal thereto (in degree): but if a person forgives and makes reconciliation his reward is due from Allah: for (Allah) loveth not those who do wrong. (42:40).
>
> 3. But indeed if any do help and defend themselves after a wrong (done) to them against such there is no cause of blame (42:41).
>
> 4. The blame is only against those who oppress men with wrong-doing and insolently transgress beyond bounds through the land defying right and justice: for such there will be a Penalty grievous. (42:42)

Aulaqi did not respond. Two days later, on January 18, 2009, Hasan sent a lengthier message discussing how the Western world views Hamas.

> Nidal Hasan wrote:
> Assalum Alaikum Sheikh Awlaki,
>
> I know your busy but please comment if the logic of this piece is accurate. am a novice at this and would like reassurance.

May Allah (SWT) reward you.

Hamas is a democratically elected Islamic organization that is trying to establish the law of God in their land. That is why they, as well as other Islamic countries are hated by the West. The Muslims should know that Hamas and other sprouting Islamic states will make mistakes and is not going to be perfect in the implementation of Shariah. The west will be sure to point these deficiencies out. However, the believers have mercy on the believers and are firm against the non-believers. Not the other way around. How is it that Israel and the U.S. can get away with so much in the way of the mischief that they create on the earth but if any Islamic group makes an error, they are ripped apart by the enemies of Islam, some of which call themselves Muslim. with that said, Hamas should be given the benefit of the doubt if any doubt exists in regards to their strategy of rocket firings in an attempt to repel the enemy. To the rest of the Muslim world the believers ask, how is it that while the weak and the. oppressed men, women and children in Gaza are pleading: "Our Lord, rescue us from the people of this tyrannous country, and appoint for us a protector from you, and appoint to us, a helper from you, that no one comes to help. Where are the Muslims? So unlike those Islamic states that seem to be choked up when an oppressive wrong is inflicted on the Muslims, Hamas helps and defends its own Muslim people. The Palestinians have sanction to fight because they have been wronged and have been driven from their homes unjustly just because they are endeavoring to be a God abiding state and won"t submit to the enemy. And although they have full right to implement the concept of an ""eye for an eye"" or ""injury for injury"" and punish the Israelis with the like of that wherewith they are being punished, in reality Hamas seems to be more similar to mosquitoes bothering a camper on a hot summer day. More of a nuisance than an actual threat as measured by the number of causalities and damage those rockets have produced. Even if the Palestinians did forgive and forget the atrocities of the unjust killings of innocent men, women, and children, Israel would continue its transgressing oppression. Hamas and other Islamic countries believe death is better then oppression and do not to fear the blame of the blamers. The blame is only against those Zionists who oppress men with wrong-doing and insolently transgress beyond bounds through the land defying truth and justice and will be held accountable. Hamas, after mutual consultation among their fellow Muslims, seeks to make ready against the Israelis what ever force and war mounts they can muster, so that they may strike terror into the hearts of their enemies and the enemy of God. Even if all that amounts to is annoying rockets that render no real damage. Their goal is to be left alone, which can only be done by ridding themselves of Israeli aggression, blockades, and oppression. Again, the Palestinians could forgive the Zioni~t regimen but that wouldn"t stop the oppression and is thus a mute point. On top of that, the Western world makes clear that it does not want Islamic rule to prevail. Again~ they make that quite clear; not only in their own lands but in the lands of the Muslims as witnessed by their mighty plotting around the world. So in the case of Israelis reckless aggression that costs the lives of innocent women,

children, and men, the law of retribution applies. It' 's a matter of survival. If a country used a nuclear weapons on a country with the intent of destroying it, it would reciprocate in a similar manner hoping it would survive. Hamas and the Muslims hate to hurt the innocent but they have no choice if their going to have a chance to survive, flourish, and deter the zionist enemy. The recompense for an evil is an evil. So, to claim that these rocket attacks go against the spirit of Islam is false. The blame is only against those who oppress men wrongly and insolently transgress beyond bounds through the land defying truth and justice. When the enemies of Allah (SWT) tried to use the Islamic teachings against prophet Muhammad (SAWS) he uprooted those palms trees and defeated them. Even if Hamas and other budding Islamic nations do not make sound decisions at times one would expect Allah (SWT) to forgive them based on their intentions to please him by establishing and defending a country that envisions obedience to Allah (SWT). A good example of this is when an expedition to attack the Meccan caravan during a holy month was made by mistake, Allah (SWT) revealed that is was a grave sin but he not only forgave them but rewarded them further stating that disbelieving in him (SWT) was an even greater sin as a warning to the non believers. Again, Hamas and other Islamic nations use different strategies to defend their land. As they mature through this difficult process they need support from the believers and expect Muslims to suspend their critical judgment and make prayers to Allah (SWT) to help them.

Aulaqi did not respond. SD-Agent [redacted] [identified each email as] "Not a Product of Interest" because they contained [redacted]

On February 16, 2009, Hasan again wrote to Aulaqi using the website application:

Nidal Hasan wrote:

Please have alternative to donate to your web site. For example, checks/money orders may be sent to .

This can assure privacy for some who are concerned.

Jazaka-Allah-Khair

About a minute later, Hasan sent a second, similar message:

Nidal Hasan wrote:

Assalum Alaikum Wa-RhamatuAllahi Wa-Barakatu,

Please have alternative methods to donate to your web site. For example, checks/money orders may be sent to .

This can assure privacy for some who are concerned and maximize the amount given.

Jazaka-Allah-Khair

About twenty minutes later, Hasan sent a third message to Aulaqi, this time about a $5,000 scholarship:

Nidal Hasan wrote:
Assalum Alaikum Wa-RhamatuAllahi Wa-Barakatahu Imam,

InshAllah, A $5,000.00 scholarship prize is being awarded for the best essay/piece entitled "Why is Anwar Al Awlaki a great activist and leader".

We would be honored if you would award the prize. If you have any questions, concerns, or potential modifications, please e-mail me.

Advertisement will be posted in the Muslim link, in the March 2009 issue.

Jazakallah Khair, VIR Nidal PS-We met briefly a very long time ago when you were the Imam at Dar al Hijra. I doubt if you remember me. In any case I have since graduated medical school and finished residency training.

SD-Analyst reviewed all three messages [redacted] and [identified] them "Not a Product of Interest." [redacted] [The next day] SD-Agent changed the [redacted] [identification] on the third message to "Product of Interest."

On February 19, 2009, Aulaqi responded for the first time to Hasan. He sent an email to NidalHasan@aol.com, the address included in Hasan's messages:

Assalamu alaykum Br Nidal,

I pray this message reaches you at the best state of emaan and health. Jazakum Allahu khairan for thinking good of me. I don't travel so I wont be able to physically award the prize and I am too "embarrassed" for a lack of the better word to award it anyway.

May Allah assist you in your efforts.

Assalamu alaykum
Your Brother
Anwar Awlaki

Aulaqi sent the email using the address al_aulaqi@yahoo.com. Later that day, Hasan replied to that address:

Al-Hamdu-leelah,

It's nice to hear your voice even if its email.

Unfortunately, when I sent the e-mail to you everyone was giving me the green light with tenative reassurances. Everything was in the process to launch the essay contest in time for the upcoming

issue of the Muslim link. Now, obstacles have been placed by Muslims in the communtity that are petrified by potential repercussions. Allah willing everything will work out in such a way that pleases Allah (SWT). You have a very huge following but even among those there seems to be a large majority that are paralyzed by fear of losing some aspect of dunya. They would prefer to keep their admiration for you in their hearts. In any case, my personal experiences have taught me that if you align yourself to close to Allah (SWT) you will likely not have many friends but pleny of hardships. Even the Prophets use to say when is the help of Allah (SWT) coming. May Allah (SWT) elevate those that please him and render useless the efforts of those that displease him; and ensure that we both are those that please him.....ameen.

PS: If you need any assistance, Allah willing I will be able to help. I believe my biggest strength is my financial situation. Of course, and this goes without saying, that everything should be legal and in accordance with the u.s. Law and Allah (SWT) knows best and is the best disposer of affairs and ultimately decides between truth and falsehood. InshaAllah, Allah (SWT) forgies us for our short coming, forbids are body from touching the Hell-Fire, allows plenty of shade on the day of reckoning, and hastens our entrance into Jannah where we will see each other (in Jannah) sipping on non-intoxicating wine in reclined thrones and in absolute and unending happiness. PS: Ilm looking for a wife that is willing to strive with me to please Allah (SWT). I will strongly consider a recommendation coming from you.

Jazaka-Allah-Khair, Sincerely, Nidal Hasan SoA(SWT), MD, MPH

SD-Agent reviewed both messages [redacted] and [identified] them "Not a Product of Interest."

On February 22, 2009, Aulaqi again emailed Hasan:

Assalamu alaykum Br Nidal,
Believe it or not I kind of felt that the contest would end up running into red tape. People in that part of the world are becoming very timid and it doesn't look it's getting any better. Thanks for the offer for help. Well it is needed but I just don't know how to do it. There are poor people, orphans, widows, dawa projects, and the list goes on. So if you have any ideas on how to get help across and in accordance to law in a climate that is strict to start with please let me know.
Tell more about yourself. I will keep an eye for a sister.

Assalamu alaykum
Anwar

Hasan replied by email that day:

Alaykum salam wa-rhamatullallahi wa-barakatu,

I will keep trying. If Allah (SWT) wants somethig to occur no one can stop it. My job is to put the effort and have patience. Your various works force the controversial issues to surface and be addressed. If there is going to be a resolution between Islam and the West the difficult issues have to be brought up.? I think this is important. It may take many generations before people realize the gift that Allah (SWT) has given them through your work. But, I see the value now and don't have to wait for your death.

In regards to pleasing Allah (SWT) I, with his mercy, am already involved in giving to the poor, orphans, widows and dawa projects. They are usually connected with the Muslim Community Center in Silver Spring MD but I do alot of work by myself because of the rigid criteria they have for giving to the poor and needy. Whether its time or money I truly believe Allah (SWT)? gives it all back and more. My goal is Jannat Firdaus and I praise and thank Allah (SWT) for giving be the ability to strive, to see the truth, to beg for his forgiveness, and ask for his guidance. If people trUly understood the peace they could have by really believing that Allah (SWT) is in control and that he is just testing to see who is the best amongs us, it would be alot' easier to see throught Shaitans promises of poverty and destruction.? I want to be with those who are the best. Imam, if you have any specific projects that you feel are important to get on their feet let me know. I will read up on them and Inshallah I will please Allah (SWT). In regards to a sister for marriage. My name is Nidal Hasan. If you google "CSTS and Nidal Hasan" you will see a picture of me. I currently reside in Silver Sping MD; 301-547-1599. I was born and raised in the U.S .. Both, of my parents are from Palestine but have both passed away (yaAllah-arhamhum). I joined the U.S. military at age 17 as an infantryman. I subsequently received a BS in Biocehmistry, Degree in medicine with residency training in psychiatry, and am just finishing up my fellowship training in Disaster and Preventive Psychiatry. During my workig career I have been a bus boy, a dishwasher, a cook, a cashier, a lab technician, a researcher, and entrepreneur. Allah (SWT) lifted the veil from my eyes about 8-9 years ago and I have been striving for Jannat Firdaus ever since. I hope, Inshallah, my endeavor will be realized. If you know someone that you feel that will be compatible and complement my endeavors to please Allah (SWT) please let me know.

Assalum Alaykum,
Nidal

SD-Analyst reviewed these two messages [redacted] [and identified] each of them "Not a Product of Interest."

Aulaqi sent no further personal email messages to Hasan.

D. Washington, D.C.: February 25 – 26, 2009

FBI Supervisory Special Agent WFO-SSA supervised CT-1, a [redacted] squad in the WFO JTTF. On or about February 25, 2009, he read San Diego's Discretionary Action lead on Hasan. Because Hasan was apparently in the U.S. military, WFO-SSA sent an EC on February 25, 2009, assigning the lead to WFO-TFO, a DCIS Special Agent who had joined the WFO JTTF in 2007. WFO-SSA also placed a paper copy of the lead on WFO-TFO's office chair.

WFO-SSA instructed WFO-TFO to conduct an "assessment." He gave him no other instructions. He did not impose a deadline. He expected WFO-TFO to take action within a reasonable time.

At that time, no written FBI policy set a deadline for completing work on Routine leads. Because FBI supervisors reviewed work assignments at quarterly file reviews, informal FBI policy required work on Routine leads to be completed within ninety days. (By comparison, FBI written policy requires that "[e]very attempt must be made to 'mitigate' Guardian incidents within the first 30 days" after assignment. [redacted] [FBI policy number redacted]

On May 27, 2009, the ninetieth day after the lead was assigned, WFO-TFO read the lead. During the ninety days between February 25 and May 27, 2009, Hasan communicated with Aulaqi five more times.

E. San Diego: February 25, 2009 – May 27, 2009

On February 28, 2009, Hasan sent Aulaqi an email attaching a document titled "Public Opinion in the Islamic World on Terrorism, al Qaeda, and U.S. Policies," and dated February 25, 2009. Hasan wrote:

> Assalum Alaikum Wa-Rhamatu-Allahi Wa-Barakatu,
>
> This well done survey sponsored by the U.S. goverment through the University of Maryland shows that most Muslims feel that US is trying to undermine Islam. It substantiates an earlier study it did as well as other studies by other organizations. I think you will find it interesting. V/R Nidal

Aulaqi did not respond. [redacted] [SD-Agent identified] this email as "Not a Product of Interest." That day, Hasan sent Aulaqi a link to a news article about Imam Yayha Hendi of the Islamic Society of Frederick, Maryland. Hasan wrote:

> FYI:? He is well known in the Greater Washington Area and serves the U.S. military as Imam for the Bethesda medical center. ?A true vision of what the government views as a good role model for all Muslims.
>
> http://your4state.com'content/fulltext/?cid=53341

SD-Agent [redacted] [identified] this email as a "Product of Interest." [redacted] [He also identified] it "Reasonably Appears to be Foreign Intelligence" because he initially believed that [redacted].

On March 3, 2009, Hasan emailed Aulaqi

> Assalum Alaikum Wa-Rhamatu-Allahi Wa-Barakatu Anwar,
> Please tell me the full amount that you would need to secure the domain fee, etc for the time period specified. I have already sent a previous request asking that different payment 'methods be used so that the full amount goes to your website and no one gets a cut. If you don't have an alternative and don't intend to get one please let me know and I can send it through PayPal.
> Jazakallah Khair,
> Nidal

Aulaqi did not respond. SD-Analyst [redacted] [identified] this email as a "Product of Interest," but "Non-Pertinent." [redacted]

On March 7, 2009, Hasan wrote Aulaqi again:

> I know your busy. Please keep me?in your rolodex in case you find me useful and?feel free to call me collect. I ask Allah (SWT) to honor those that please him in this life and the next and to render the efforts useless of those who strive against the most Gracious. InshAllah we will see each other later.
>
> PS: I really enjoyed the story about the?brave person?who stated "I dont fear any man" but Prophet Muhamad (SAW) said you will tremble when you see this man and when he saw the man he indeed trembled.
>
> JazakAllah Khair, Nidal Hasan, MD, MPH
> 9304 Cedar Lane
> Bethesda Maryland
> 20814 (301) 547-1599

Aulaqi did not respond SD-Analyst [redacted] [identified] this email as "Reasonably Appears to be Foreign Intelligence" because [redacted]

Almost two months passed before Hasan wrote to Aulaqi again.

On May 17, 2009, the U.S. Army promoted Hasan from Captain to Major.

On May 25, 2009, Hasan visited Aulaqi's website and posted a new message, which the website automatically forwarded to al_aulaqi@yahoo.com. We do not know why Hasan used the website instead of the email address Aulaqi had disclosed to him. By that time, the website had been updated, and the messages were rendered in a different format when emailed. The message read:

Your name: Nidal Hasan
Email: NidalHasan@aol.com

Message:
Brother Anwar don't fear the blame of the blamers'

When I read this verse (below) I think of you. Most of us have truned back for fear or the for zina of this life. We have thus suspended our critical Judgment for a small price.

Allah (SWT) makes it clear that most wont believe and of those that do; the ones who struggle for his cause are greater in his sight then those who sit back and pray.

O you who believe! Whoever from among you turns back from his religion (Isli?¢¢m), Alli?¢¢h will bring a people ([like Anwar Al Awalaki] whom He will love and they will love Him; humble towards the believers, stern towards the disbelievers, fighting in the Way of Alli?¢¢h, and never fear of the blame of the blamers. That is the Grace of Alli?¢¢h which He bestows on whom He wills. And Alli?¢¢h is AllSufficient for His creatures' needs, All-Knower.

Your Brother Nidal

Aulaqi did not respond. [redacted] SD-Analyst [identified] this email as "Not Pertinent" and "Not a Product of Interest "

F. Washington, D.C.: May 27, 2009

On February 25, 2009, WFO-SSA had assigned the Hasan lead to WFO-TFO and asked him to perform an assessment. Under informal FBI policy, Routine leads were to be closed or transformed into a case within ninety days. On May 27, 2009 – ninety days after WFO-SSA assigned the lead – WFO-TFO read it.

WFO-TFO noticed San Diego's misinterpretation of the DEIDS notation "Comm Officer." WFO-TFO had known others to interpret that notation to mean Communications Officer.

WFO-TFO searched DEIDS to confirm the military status and duty location of Nidal Malik Hasan. He searched the DoD Joint Personnel Adjudication System and learned that Hasan had a Secret clearance and had recently passed a clearance re-investigation. WFO-TFO searched the FBI Telephone Applications database and found no links between the telephone number shown in Hasan's DEIDS report and any "target" numbers. WFO-TFO's search of the FBI's Automated Case Support (ACS) system using Hasan's email address returned only San Diego's EC.

WFO-TFO did not search DWS-EDMS, IDW, or DaLAS. Although he was a member of a [redacted] counterterrorism squad, he says he did not know that DWS-EDMS existed. He believes that no one at WFO CT-1 other than an Intelligence Analyst, WFO-Analyst, had access to DWS-EDMS until after the Fort Hood shootings. He had previously reviewed [redacted] [FBI-acquired communications], but only in ACS.

WFO-TFO contacted DoD-Analyst, a non-JTTF DCIS Intelligence Analyst based in Arlington, Virginia. He asked DoD-Analyst to obtain records on Hasan from the Defense Manpower Personnel Center in Monterey, California. She emailed the records to him.

WFO-TFO had limited access to DoD personnel files. The files he could review, which DoD-Analyst provided to him, consisted of Hasan's Electronic Personnel File, which totaled approximately 65 pages. The file included, among other things:

- Academic Evaluation Reports and Academic Transcripts from the Uniformed Services University for Health Sciences dating to 1999;
- Six Officer Evaluation Reports (OERs) covering June 2003 to June 2008; and
- Promotion Orders.

The OERs contained almost uniformly positive evaluations of Hasan by his superior officers. For example, the Department Chair of Psychiatry at Walter Reed wrote that Hasan's research on Islamic beliefs regarding military service during the Global War on Terror "has extraordinary potential to inform national policy and military strategy." There were comments that Hasan deserved promotion. The Promotion Orders showed that Hasan had been promoted from Captain to Major ten days earlier, on May 17, 2009. The only derogatory information that WFO-TFO found was an indication that Hasan had not passed his Army Physical Fitness Test between July 2007 and June 2008.

WFO-TFO did not have access to any files maintained locally by Hasan's command. Those files revealed that the program directors overseeing Hasan during his residency and fellowship at Walter Reed and the Uniformed Services University of the Health Sciences ranked him in the bottom 25 percent. He was placed on probation and remediation and often failed to meet basic job expectations such as attendance at work and being available when he was the physician on call. WFO-TFO also did not have access to a memorandum to the National Capital Consortium's Credentials Committee, dated May 17, 2007, faulting Hasan's professionalism and work ethic, which was leaked to the media in the aftermath of the Fort Hood shootings.

Based on what he read, WFO-TFO believed that Hasan's communications with Aulaqi were relevant to his research on Islam and the military. WFO-TFO decided that Hasan was not involved in terrorist activities. He took no further investigative action.

WFO-TFO then consulted WFO-SSA. WFO-SSA did not ask whether Aulaqi had responded to Hasan's messages or whether there were any further emails between Hasan and Aulaqi. He did ask whether WFO-TFO had checked all of the FBI databases. WFO-TFO said that he had.

WFO-SSA and WFO-TFO discussed whether an interview of Hasan or his supervisor would be appropriate. They believed that any overt investigative steps would do more harm than good. Given the [redacted] origin of the information [redacted], WFO-SSA and WFO-TFO believed that interviewing Hasan would jeopardize the [Aulaqi investigation.] [redacted] They could think of no way to interview Hasan without

disclosing the FBI's access to the messages, [redacted] which would harm the prime interest – San Diego's investigation of Aulaqi. Neither WFO-SSA nor WFO-TFO believed a pretext interview of Hasan would be appropriate.

WFO-SSA and WFO-TFO also believed that the "least intrusive means" requirement precluded an interview of Hasan or contact with his superior officers. They knew that an interview is a permissible technique for an assessment. They believed, however, that Hasan's messages were relevant to his research and that an interview of Hasan was unnecessary. WFO-TFO believed that an interview would require notification to Hasan's commanding officer; that the interview would probably be briefed up the Army chain of command; and that this would harm Hasan's career. As a result, WFO-TFO considered an interview highly intrusive.

WFO-SSA agreed with WFO-TFO's conclusions – including the determination that Hasan was not a threat – and believed that no further action was appropriate.

Neither WFO-SSA nor WFO-TFO considered approaching Hasan as a potential confidential human source. In their view, a good source had access to information. The two messages to Aulaqi contained no indication that Hasan could provide useful information.

After these actions and discussion – which took place within the span of four hours on the same day, May 27, 2009 – WFO-TFO wrote and WFO-SSA approved the WFO EC response to the lead. After outlining the information gathered, the WFO response concluded:

> 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 messages, WFO does not currently assess Hasan to be involved in terrorist activities. WFO will re-assess this matter if additional information is identified.

Although the response stated that WFO had "reviewed FBI and Department of Defense databases and record systems" and that Hasan's messages were "to date, unanswered," WFO had not checked DWS-EDMS, [IDW, and DaLAS] to determine whether this was correct.

WFO sent the response to San Diego, ITOS 1 (CONUS 6 and CONUS 2), and the Baltimore Field Office (because Hasan's home address was located in Baltimore's Area of Responsibility).

G. San Diego: May 27, 2009 – June 11, 2009

On May 31, 2009, Hasan visited Aulaqi's website and sent another message to him:

> Assalum Alaikum Wa-RhamatuAllahi Wa-Barakatuhu brother Anwar; InshAllah Khair,
>
> I heard a speaker defending suicide bombings as permissible and have been using his logic in debates to see how effective it really is.

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.

For example, he reported a recent incident were an American Soldier jumped on a grenade that was thrown at a group of soldiers. In doing so he saved 7 soldiers but killed himself. He consciously made a decision to kill himself but his intention was to save his comrades and indeed he was successfull. So, he says this proves that suicide is permissible in this example because he is a hero. 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 know 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 successfull. His intention was to save his people/fellow soldiers and the stategy was to sacrifice his life.

The logic seems to make sense to me because in the first example he proves that suicide is permissible i.e. most would consider him a hero. I don't want to make this to long but the issue of "collateral damage" where a decision is made to allow the killing of innocents for a valuable target. If the Qur'an it states to fight your enemies as they fight you but don't transgress. So, I would assume that suicide bomber whose aim is to kill enemy soldiers or their helpers but also kill innocents in the process is acceptable. Furthermore, if enemy soldiers are using other tactics that are unethical/unconscionable than those same tactics may be used.

JazakAllah Khair, P.S. We miss hearing from you'

Aulaqi did not respond. [redacted] SD-Analyst reviewed this email and [identified] it [redacted] "Needs Review." SD-Agent then reviewed the email and [redacted] [identified] it "Not a Product of Interest" and "Not Pertinent" because he read it as [redacted]

H. San Diego and Washington, D.C.: June 11, 2009 – June 15, 2009

On or about June 11, 2009, SD-Agent reviewed WFO's response to the lead. He was disappointed. He believed the assessment was "slim." The information about Hasan's personnel files was unhelpful, because personnel files typically contain praise. The reasons for not interviewing Hasan seemed to be weak excuses for not taking additional action.

Despite WFO's offer to "re-assess this matter if additional information is identified," SD-Agent and SD-Analyst did not check DWS-EDMS for additional messages between Hasan and Aulaqi.

SD-Agent showed the response to SD-TFO2 and SD-TFO3. They agreed that the assessment was inadequate SD-TFO2 found it hard to believe that a DoD representative had written the response. SD-TFO3 found the response so strange that he suspected that Hasan was a confidential source for WFO.

SD-Agent decided to follow-up with WFO. He had taken that step only once before in his career, when another Field Office had failed to take action on a lead SD-Agent knew his FBI counterpart WFO-SSA. Instead of contacting him, SD-Agent put SD-TFO3 in what SD-Agent considered the "uncomfortable position" of asking a fellow DCIS Agent why he did not take further action. SD-Agent took this approach to avoid being, in his words, "the heavy" in dealing with a DCIS Agent in another JTTF. He did not consider bringing the issue to his supervisor, to WFO-SSA, or to anyone at Headquarters.

SD-TFO3 contacted a DCIS program manager to ask for background information on WFO-TFO. The program manager spoke positively about WFO-TFO.

SD-TFO3 called WFO-TFO on June 11, 2009. WFO-TFO said he was unable to talk because he was occupied with a shooting incident at the Holocaust Museum. He said they could talk as soon as he was available.

On the following day, June 12, 2009, SD-TFO3 emailed WFO-TFO. The full text of his message reads:

> [WFO-TFO],
>
> We just received your response to our lead on 415F-SD-60934, Subj: Anwar Nasser Aulaqui re: Assessment of Nidal Malik Hasan (a US Army Captain, Medical Doctor, Walter Reed).
>
> The case agent wanted me to follow up on this commenting: The response looks a little slim, i.e. limited probing into this individuals background, no contact w/ command and no interview of Hasan.
>
> We were wondering if we were missing something, i.e. we need to read between the lines (Hasan is a friend of WFO)?
>
> [SD-TFO3], Special Agent
> DCIS San Diego Resident Agency

WFO-TFO discussed the email with WFO-SSA. WFO-SSA did not consider contacting SD-Agent. He left the response to WFO-TFO, and advised him to "be nice" in responding. WFO-TFO sent the following email to SD-TFO3 that afternoon:

> [SD-TFO3]: Sorry I couldn't get back to you on a hard line yesterday. I never made it into the JTTF scif as I (along with most everyone else) was pulled to work the Holocaust Museum shooting.
>
> Please note that I looked into HASAN as a result of a discretionary lead, "for action as deemed appropriate." From your email, I assume SD desired a deeper investigation. However, since HASAN's contact with Aulaqi [redacted], I did not contact him nor his command officials directly. I did however, determine that HASAN was conducting US Army sponsored research that was online with the questions he sent Aulaqi.

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 email messages, WFO does not currently assess HASAN to be involved in terrorist activities. WFO will re-assess this matter if additional information is identified.

To my knowledge, HASAN is not a CHS nor "a friend of WFO." If you have additional information regarding HASAN's links to terrorism or request any specific action, please share and we will re-assess. BTW, HASAN lives in Baltimore's AOR but works in WFO's AOR. I copied Baltimore on the response EC.

SD-TFO3 forwarded WFO-TFO's email to SD-Agent, with the following cover message:

[SD-Agent],

RE: E-mail from Hasan to Aulaqi

This will not be a satisfying read. That said, I've asked the question of WFO and here's their answer.

A few days later, on or about June 15, 2009, SD-Agent visited SD-TFO3 to discuss WFO-TFO's email. SD-Agent was upset. He again asked SD-TFO3 to call WFO-TFO to find out why WFO had done nothing further.

According to SD-TFO3, he called WFO-TFO again. SD-TFO3 told him that, upon receiving a lead like this one, San Diego would have conducted, at the least, an interview of the subject. SD-TFO3 recalls that WFO-TFO replied, in effect (paraphrased, not a quotation): "This is not SD, it's DC and WFO doesn't go out and interview every Muslim guy who visits extremist websites. Besides, this guy has a legitimate work related reasons to be going to these sites and engaging these extremists in dialogue. WFO did not assess this guy as a terrorism threat." SD-TFO3 also recalls that WFO-TFO indicated that this subject is "politically sensitive for WFO."

WFO-TFO, on the other hand, does not recall receiving another telephone call from SD-TFO3. The FBI does not have records of SD-TFO3's telephone calls from the San Diego JTTF.

According to FBI written policy, "the receiving office" – here, WFO – "will decide what, if any, action to take" on a Discretionary Action Lead. MAOP § 10.2.9(1)(a)-(c). SD-Agent and SD-TFO3 dropped their inquiries to WFO. They believed they had done all they could do.

I. San Diego: June 16, 2009 – June 17, 2009 and After

On the next day, June 16, 2009, [redacted] Hasan [sent his] final message to Aulaqi. Hasan sent the message via the website. Its full text read:

Assalum Alaikum Wa-RhamatuAllahi Wa-Barakatuhu,

I listened to a lecture that made a parallel between Iblis and the People of the book and was wondering if it was consistent with what the Quran teaches. He basically stated that Allah (SWT)

speaks the truth and should always be obeyed. He told the story of how Allah (SWT) told Adam (AS) to take Shaitan as an enemy and toldy him to stay away from the tree. Shaitan told Adam that he was his well wisher and the only reason the tree was denied him because it would make him an angel or live forever. So Adam listened to Shaitan and neglected the heedings of his lord. He goes on to say that Allah (SWT) warns us not to take the people of the book as protecting friends (aulia) and the lecturer stated that if we ignore Allah (SWT) like Adam we will have no exuse if we end up in hell fire because of the advice given by the people of the book. He explains that some of the people of the book are sincere in their advice but are ignorant and if you listen to sincere ignorant advice over Allah (SWT) you fall at your own peril. V/R Nidal

SD-Analyst reviewed the email and [redacted] [identified] it "Not a Product of Interest" and "Not Pertinent."

[redacted] [By] June 16, 2009, the date of Hasan's last message, [SD-Agent and SD-Analyst had reviewed more than 20,000 electronic documents as part of the investigation – on average 1,375 per month, or 65 to 70 per work day.] [redacted]

The weighty pace of activity on the [Aulaqi investigation] [redacted] continued after Hasan's last message. On July 1, 2009, the Aulaqi investigation shifted from "315" to "415" designation as part of an administrative revision of case classification codes. [redacted] As of November 5, 2009, the date of the Fort Hood shootings, [redacted] [SD-Agent and SD-Analyst had reviewed more than 29,000 electronic documents – on average 1,525 per month, or 70-75 per work day.]

The FBI took no further action concerning Hasan until November 5, 2009.

J. Aftermath

Effective July 15, 2009, the U.S. Army transferred Hasan from Walter Reed Army Medical Center to the Darnall Army Medical Center at Fort Hood, Texas. Fort Hood is the Army's staging area for deployment to combat zones.

On August 16, 2009, Hasan reported to the Killeen Police Department that a fellow Army soldier, John Van De Walker, had vandalized his car. Police arrested Van De Walker on October 21, 2009. According to newspaper reports, he confessed that Hasan's bumper sticker, which referenced Allah, offended him. He used a key to scratch Hasan's car.

On July 31, 2009, Hasan purchased a Herstal FN-57 handgun from Guns Galore in Killeen, Texas.

In October 2009, the U.S. Army notified Hasan that he would be deployed to Afghanistan in November 2009.

On November 5, 2009, Hasan entered the Fort Hood deployment center, where he shot and killed thirteen people and wounded 43 others. Nearly five months had passed without any further known personal communications between Hasan and Aulaqi (see Chapter 7).

In the wake of the shootings, Aulaqi publicly hailed Hasan as a role model for his attack on fellow soldiers, stating: "Who would object to that?"

SD-Agent continued to [redacted] [investigate Aulaqi] with the assistance of other San Diego JTTF members and ITOS Analysts. SD-Analyst transitioned to a domestic terrorism squad, which he had requested prior to the Fort Hood shootings. WFO-SSA transferred from WFO to [redacted] [another FBI] Field Office, where he is a member of [redacted] [its] JTTF. WFO-TFO has returned to DCIS as Special Agent in Charge of [one of its offices.] [redacted]

[redacted] [In mid]-2011, an FBI [redacted] report documented an interview with an FBI subject [redacted] in which [redacted] [the subject] claimed to have met Aulaqi after the Fort Hood shootings. According to [redacted] [the subject], Aulaqi told him that Hasan "had contacted him via the Internet and had asked what he could do to help Muslims" and that Aulaqi had "advised Hasan that since he was an American soldier, he should kill other American soldiers." According to [redacted] [the subject], Aulaqi said he had given Hasan "permission to carry out his attacks at Fort Hood."

Although Hasan did contact Aulaqi via the Internet, we found no evidence, direct or indirect, that Aulaqi made these purported statements to Hasan (see Chapter 7). The evidence shows instead that Aulaqi did not even respond to Hasan's first message and its question about whether the acts of Muslim soldiers who had killed other soldiers could be reconciled with the Quran. The WASHINGTON POST reported on November 16, 2009, that in an interview with a Yemeni journalist, Aulaqi "said that he neither ordered nor pressured Maj. Nidal M. Hasan to harm Americans...."

On September 30, 2011, the White House and the State Department confirmed reports that Anwar Nasser al-Aulaqi had been killed in Yemen.

Chapter 7:

Review of FBI Data Holdings on Nidal Malik Hasan

A. Introduction and Conclusions

We conducted, to the degree possible given the criminal investigation and prosecution of Hasan, an independent investigation of all FBI data holdings to assess:

(1) Whether contemporaneous searches of FBI data holdings on December 17, 2008 (the date of Hasan's first message); January 7, 2009 (the date of San Diego's lead); May 27, 2009 (the date of WFO's response to San Diego); or November 4, 2009 (the day before the shootings) would have revealed other information about Hasan;

(2) Whether there was any evidence of other electronic communications between Hasan and Aulaqi;

(3) Whether surveillance of Hasan's email in the weeks before the shootings would have produced any actionable evidence of imminent violence or other wrongdoing; and

(4) Whether the FBI's post-shooting review of FBI and USIC data holdings on Hasan was accurate and complete.

Our investigation concludes that:

(1) Contemporaneous searches of FBI data holdings would not have revealed any suggestion of impending wrongdoing by Hasan or any other actionable information about Hasan;

(2) There is evidence of electronic communications between Hasan and Aulaqi other than the eighteen messages [reviewed by SD-Agent and SD-Analyst] [redacted] but those communications were generic mass "news" emails that Aulaqi sent to all persons who subscribed to his website's email list;

(3) Surveillance of the NidalHasan@aol.com email account in the weeks preceding the shootings would not have produced any actionable evidence of imminent violence or other wrongdoing; and

(4) The FBI's post-shooting review of FBI and USIC data holdings on Hasan was professional, comprehensive, accurate, and complete. (We did not examine, and

do not express any views on, other elements of the FBI's post-shooting investigation of Hasan.)

B. Contemporaneous Searches of FBI Holdings

To assess whether the FBI possessed other information about Hasan as of December 17, 2008 (the date of his first message); January 7, 2009 (the date of the lead); May 27, 2009 (the date of WFO's response to San Diego); or November 4, 2009 (the day before the shootings), we searched the FBI's primary data holdings: ACS, DWS-EDMS, IDW, and DaLAS.

ACS. We searched all ACS holdings as of November 5, 2009, using the search terms [redacted] Our search returned only San Diego's EC of January 7, 2009, setting the lead on Hasan.

DWS-EDMS. We searched all DWS-EDMS holdings as of November 5, 2009, using the search terms NidalHasan@aol.com [redacted]

A full text search using the term NidalHasan@aol.com returned [redacted] [some of the] known communications between Hasan and Aulaqi. [redacted] The messages sent via Aulaqi's website included the search term, but adjacent to other characters, as <NidalHasan@aol.com>. As a result – and underscoring the limitations of literal search technologies – a full text search did not return those messages.

A "participant" search for NidalHasan@aol.com – which is limited to iterations of email accounts – avoided the full text search limitations and returned [all messages between Hasan and Aulaqi that SD-Agent and SD-Analyst reviewed.] [redacted]

The search [redacted] returned [redacted] [all messages between Hasan and Aulaqi that SD-Agent and SD-Analyst reviewed]; and one match from [redacted] [an unrelated investigation] (which we discuss below).

The [redacted] matches for [redacted] included the [redacted] matches for [redacted]. We reviewed each of the remaining [redacted] matches. [redacted] None involved the Nidal Hasan at issue.

SD-Agent conducted a "participant" search of DWS on or about January 7, 2009, using NidalHasan@aol.com. That search returned the message Hasan sent to Aulaqi on January 1, 2009. If SD-Agent or SD-Analyst had searched DWS – and later, DWS-EDMS – using the only

other identifying search terms known at the time [redacted] then or at any other time before November 5, 2009, they would have found only one relevant product other than [the messages between Hasan and Aulaqi that SD-Agent and SD-Analyst reviewed] [redacted]

Our search revealed the name Nidal Hasan in the text of a March 29, 2006, [redacted] mailing list message [redacted] [that the FBI acquired in] an investigation unrelated to Aulaqi. The post is titled "Imam Needed for Walter Reed Army Medical Center." Its text reveals that Nidal Hasan is a member of the military by referencing Walter Reed and including one of Hasan's military email addresses as a contact. The person who posted the text appears to have copied it from another online source – probably an Internet post by Hasan.

The full text, which the reviewing Agent on that separate [redacted] [investigation] properly tagged "Non-Pertinent,"reads:

> Assalamu 'alaykum was rahmatullah,
>
> Brothers and sisters,
>
> Walter Reed Army Medical Center is in need of an Imam for jumua'ah prayers held at WRAMC in Washington, DC, as well as to console/make dua for Muslim patients in the Medical Center.
>
> This has the option of becoming a full-time position, based on experience and educational qualification.
>
> For more information, please contact br. Nidal Hasan at Nidal.Hasan@NA.AMEDD.ARMY.MIL.
>
> May Allah bless your efforts, wassalama 'alaykum,

DaLAS. We also searched all DaLAS holdings as of November 5, 2009, using the search terms NidalHasan@aol.com [redacted]

These searches returned [redacted] matches. We reviewed each file. One file was the [redacted] "Imam Needed" mailing list message noted above, which had been uploaded to DaLAS on August 5, 2008, in a case unrelated to Hasan. Because of potential attorney-client privileged information, access to that file was restricted to specified users.

None of the other files involved the Nidal Hasan at issue here. As discussed below, as of November 5, 2009, DaLAS did hold one other non-pertinent product involving Hasan; but that product could be tied to Hasan only through an email address that the FBI identified after the shootings. A search of DaLAS using all potential search terms known to San Diego and WFO prior to the shootings could not have returned that item.

C. FBI Searches of FBI Data Holdings

In the immediate aftermath of the Fort Hood shootings, STAS conducted a search of all FBI data holdings to identify all information in the FBI's possession involving Hasan. STAS identified the [redacted] "Imam Needed" post that we located in our search of DWS-EDMS.

The Electronic Communications Analysis Unit (ECAU) and the Digital Media Exploitation Unit (DMX) later conducted a second search in support of the criminal investigation and prosecution. Prior to this search, the U S. Army Criminal Investigation Division (CID) had supplied ECAU and DMX with all content and metadata for five DoD email addresses associated with Hasan. ECAU had independently determined that, in addition to the NidalHasan@aol.com account, Hasan had a second AOL account with email and instant messaging (AIM) addresses as well as a Yahoo! email account.

FBI Analysts checked these nine email/AIM addresses against four FBI databases (ACS, Clearwater, DaLAS, and DWS-EDMS) as well as several USIC databases The Analysts found [redacted] matches [redacted] in FBI holdings.

[redacted] [One] match on a search for Nidal.Hasan@NA.AMEDD.ARMY.MIL, returned the "Imam Needed" post [noted above] in DWS-EDMS and DaLAS.

[redacted] Another match, on a search for Hasan's other AOL email address, was located in DaLAS on a forensic image of a computer hard drive that the FBI's Newark Division had seized in 2007 pursuant to a criminal warrant in a tax case. This product is also innocuous. It shows that, on February 10, 2005, Hasan had used his other AOL address to visit a non-Jihadist web forum and post a question about the Quran's prohibition on intoxicants. The full text reads:

> Asssalum wa Alakum; I discovered Islam 2 years ago and have been building my knowledge base of the Quaran and Sunna. My question is concerning the verse in the Quaran that refers to intoxicants and the multiple hadiths that indicate the prohibition of its use. Perhaps if a islamic leader took charge we would have mediations that seve as great pain relievers as well as anti anxiety medications that arent [sic] intoxicants. However, the best materials we have now are intoxicants ie: valium, ativan, percocet, morphine etc. Should physicians be prescribing these even if the prophet SAWS stated more or less that he hoped whoever takes an intoxicant for medication purposes doesn't [sic] get better.

Conclusion: Based on our review, we conclude that contemporaneous searches of FBI data holdings on any date between December 17, 2008, and November 4, 2009, would not have disclosed any other actionable information about Hasan.

D. Evidence of Other Electronic Communications Between Hasan and Aulaqi

In the aftermath of the Fort Hood shootings, the FBI obtained access to the existing contents of Hasan's known private and military email accounts. We reviewed the content of Hasan's active private account, NidalHasan@aol.com. We also interviewed FBI personnel tasked with reviewing Hasan's other email accounts and the contents of his computer hard drive and telecommunications devices. There is no certainty that the contents of these accounts and media provide a complete history of Hasan's communications prior to the shootings. Most email systems delete sent messages automatically or after a specified time period, and users may delete messages as they see fit and set rules to delete messages after specified time periods. Moreover, email deleted from Hasan's New Mail, Old Mail, Sent Items, and Trash folders on AOL would not normally be recoverable because AOL regularly purges its systems of deleted email. With these limitations in mind, neither the extensive ECAU/DMX review nor our relatively limited review identified any other personal contact between Hasan and Aulaqi.

Our review of the NidalHasan@aol.com account disclosed, however, that Hasan did receive other electronic communications from Aulaqi. None of these communications was personal or specific to Hasan. Instead, at some date prior to December 21, 2008 – at about the same time he sent his first message to Aulaqi – Hasan had subscribed to a Google FeedBurner list to receive "Anwar Al Awlaki On-Line" email updates, by which he and an unknown number of other subscribers received irregular mass email announcements, articles, and other statements from Aulaqi.

The email updates were issued to FeedBurner – and, in turn, to NidalHasan@aol.com and other subscribers – from the email account donotreply@anwar-alAulaqi.com. [redacted] The FBI did not acquire these emails until after the Fort Hood shooting. [redacted]

Through his subscription, Hasan received and retained at least 29 email updates from Anwar al Awlaki On-Line. The subjects of these updates varied and included, for example:

- A December 20, 2008, email, titled "Salutations to al-Shabab of Somalia," offered congratulations to al-Shabaab "for your victories and achievements," asked Allah to "guide you and grant you victory," and noted that "[o]nly Allah knows that if my circumstances would have allowed I would not have hesitated in joining you and being a soldier in your ranks";

- A January 5, 2009, email provided Word and .pdf copies of Aulaqi's article "44 Ways of Supporting Jihad';

- A July 14, 2009, email discussed "Fighting Against Government Armies in the Muslim World," challenging the Muslims "fighting on behalf of America against the mujahideen in Pakistan, Somalia and the Maghrib.... What kind of twisted figh[t] is this? The blame should be placed on the soldier who is willing to follow orders

whether the order is to kill Muslims as in Swat, bomb Masjids as with the Red Masjid, or kill women and children as they do in Somalia, just for the sake of a miser salary. This soldier is a heartless beast, bent on evil, who sells his religion for a few dollars. These armies are the number one enemy of the ummah. They are the worst of creation. Blessed are those who fight against them and blessed are those shuhada who are killed by them."

We reviewed Hasan's messages to Aulaqi in the added context of these mass-mailed messages from Aulaqi. We found no direct connection between the personal messages and the mass-mailed ones.

Conclusion: Upon completion of our review of FBI data holdings and interviews, we found no evidence that, in the year preceding November 5, 2009, Hasan and Aulaqi engaged in any person-to-person electronic communications other than in the 18 known messages [redacted].

E. Post-Shooting Review of Seized Electronic Records and Media

We examined all available email messages associated with NidalHasan@aol.com that the FBI obtained during the investigation of the shootings. For the reasons noted above, the available email does not likely represent every email that Hasan sent and received using the account.

We read every existing email – 184 messages – that Hasan sent and received in the two weeks before November 5, 2009. We found no obvious evidence of the intentional deletion of email in those two weeks. We concluded that access to that email would not have provided any evidence of an imminent violent act.

The available email received by Hasan in those two weeks consisted primarily of unsolicited messages ("spam"); one of the Aulaqi mass newslist emails discussed above; and emails from other subscription news alerts (Google Alert, for "sharia"); RSS feeds (Islamistwatch.org), and newslists (islamicreliefusa.org, the Middle East Forum, newsrealblog, RadicalIslam.org,). The subjects of these emails also varied; for example:

- An article entitled "The Third Jihad" from RadicalIslam.org
- An article entitled "Exporting American anti-Americanism to Muslim world" from the Middle East Forum website
- A blog entry entitled "Imam Killed in FBI Shootout Sat on Board of Muslim Lobby Group MANA," also from the Middle East Forum website

Hasan's only existing personal emails in that two-week period were businesslike messages to and from U.S. Army representatives concerning his posting to Afghanistan and routine administrative and scheduling matters. We also found two emails exchanged with his brother, Anas Hasan. On October 30, 2009, Hasan wrote to Anas:

Assalum Alaıkum Wa-RhamutaAllahı Wa-Baragatuhoo Wa-Maghfıratu,

Anas, I'm not sure ıf Eyad told you but I am leavıng for Afghanıstan next month. I wıll be leavıng sometıme next week to vısıt Eyad and hıs famıly ın Vırgınıa and than head towards Georgıa for some fınal traınıng before flyıng out. In any case, I have transferred 21,000 dollars that I owe you ınto the busıness account. We are now even- of course you take the 4,000 that you have of mıne also for a total of 25,0000. Please take ıt out ASAP, I don't lıke thıngs floatıng and ıf you lose ıt for any reason ıt's your fault..

I have fılled out a power of attorney so that you may handle my affaırs ın case I need somethıng done durıng the 6 months I'm ın Afghanıstan or ıf I dıe, etc- I'm not sure ıf ıt wıll work for everythıng but I wıll gıve a copy to Eyad to hold when I vısıt hım. In the event that I am ıncapacıtated or not able to use my money/property ı.e. captured by the enemy please donate my money/property to the poor as soon as possıble- use your judgment but you know I'm tryıng to maxımıze by rewards. If I happen to dıe obvıously splıt ıt accordıng to the Islamıc ınheritance law and gıve the maxımum allowable amount to a charıty/sadaqa jarıah etc- I thınk ıts 1/3 of my wealth. I am not aware of any psychıatrıst that have dıed ın Iraq/Afghanıstan by enemy fıre however ıt's always good to be prepared.

This message would raise suspicion only in hindsight. Read in the context of Hasan's impending deployment to Afghanistan, the message appears innocuous and the likely act of a soldier about to be deployed to a combat zone

On November 1, 2009, Anas sent Hasan an email titled "Cair: Houston Texas Office" that included only a website link. The link provides an online form to report any hate crime or incident of bias, profiling, or other discrimination to the Council on American-Islamic Relations' Houston office. This message may relate to John Van De Walker's vandalism of Hasan's car in August 2009.

In addition to reviewing every available email sent and received by Hasan in the two weeks prior to the shootings, we searched all available email in his AOL account using a series of potentially relevant search terms (including, among others, imam, jihad, gun, handgun, pistol, Herstal, Five-Seven, FN, FN-57). Our searches returned no emails containing those search terms.

Conclusion: Electronic surveillance of the NidalHasan@aol.com email account in the weeks preceding the shootings would not have produced any actionable evidence of imminent violence or other wrongdoing.

Part Two

Analysis of FBI Actions

The Terms of Reference asked Judge Webster to examine "whether the actions taken by the FBI were reasonable under the circumstances known at the time." Our analysis of those actions cannot proceed from what we now know about Nidal Malik Hasan. Hindsight has uses, but it is not an appropriate tool for assessing the reasonableness and adequacy of actions taken without its benefit. Our review is based on information known or available to the FBI at the time the actions were taken.

We also recognize 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 Chapter 3, the FBI's governing authorities limit its ability to disseminate information acquired using FISA and require Agents and Task Force Officers to use the "least intrusive means" in conducting assessments and investigations. As discussed below, the FBI's information technology and document review workflow did not guarantee that all foreign intelligence would be identified in DWS-EDMS.

Finally, we recognize 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 choose not to speculate. We examine instead the reasonableness of what did happen, in order to identify and recommend, when appropriate, better and corrective policies and practices for the future. We discuss those recommendations in Part Three.

We conclude that, working in the context of the FBI's governing authorities and policies, operational capabilities, and the technological environment of the time, individuals who handled the Hasan 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 Agent, Analyst, and Task Force Officer who handled the Hasan 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 conclude instead that these committed 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 electronic information.

Chapter 8

Knowledge and Information Sharing

We begin by reviewing the FBI's understanding of violent radicalization. We then discuss what the FBI knew about Aulaqi and Hasan on January 7, 2009, when the San Diego JTTF set the lead to the Washington, D.C., JTTF (WFO), and on June 16, 2009, the date of Hasan's last message to Aulaqi. We also consider why the FBI did not share the Hasan information or the opening of the Hasan assessment with the Department of Defense (DoD).

A. The FBI's Understanding of Violent Radicalization (Chapter 1)

The FBI's understanding of violent radicalization is consistent with the contemporary views of the psychiatric community.

Before the events reviewed in this Report, the FBI had provided training on its radicalization model to Agents, Analysts, and Task Force Officers, including all personnel involved in the Hasan assessment. As discussed in Part Three, that training has expanded in the aftermath of the Fort Hood shootings.

B. The FBI's Knowledge About Anwar al-Aulaqi (Chapter 5)

As of January 7 and June 16, 2009, the FBI knew Anwar al-Aulaqi as an anti-American, radical Islamic cleric and the subject of a Tier [redacted] FBI counterterrorism investigation. San Diego believed [redacted] that Aulaqi was [developing ambitions beyond radicalization] [redacted]. WFO viewed him at that time 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. Public awareness of the threat posed by Aulaqi is an even more recent development.

San Diego's lead reasonably described the FBI's knowledge about Aulaqi as of January 7, 2009.

C. The FBI's Knowledge About Nidal Malik Hasan (Chapters 6 and 7)

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 (see Part One, Chapter 7). That knowledge justified an assessment of Hasan.

The FBI's knowledge grew, or should have grown, as San Diego 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 in May 2009 and San Diego reviewed WFO's assessment in June 2009.

The totality of that knowledge was limited. The FBI did not have access to all DoD records on Hasan, but only the limited information accessible by DoD personnel assigned as TFOs to San Diego and WFO. As a result, the FBI did not have direct access, until after the Fort Hood shootings, to the disturbing contents of Hasan's personnel files at Walter Reed Army Medical Center and the Uniformed Services University of the Health Sciences or to (among other things) Hasan's medical licensing records.

D. Information Sharing

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

1. Notice of the Hasan Assessment (Chapter 6)

Prior to the Fort Hood shootings, the FBI had no written policy on advising DoD about counterterrorism assessments or investigations of members of the U.S. military, DoD civilian personnel, or others with known access to DoD facilities. FBI Field Offices informally shared information with DoD on a regular basis when these individuals became subjects of assessments or investigations. However, there was no formal procedure and no formal requirement to advise DoD about these assessments and investigations.

When San Diego set the lead to WFO, the FBI knew only that an individual said to be named Nidal Hasan had contacted Aulaqi from the Washington, D.C., area and that a U.S. Army officer named Nidal Malik Hasan worked in Washington, D.C. San Diego did not know with certainty that a U.S. Army officer had contacted Aulaqi until receiving WFO's assessment five months later.

San Diego's EC also set an Information Only ("read and clear") lead to International Terrorism Operations Section (ITOS) 1, Continental United States (CONUS) 6, which oversees the San Diego JTTF's intelligence collection and investigative efforts. SD-Agent's cover email to ITOS 1, CONUS 6 recommended not disseminating the information as an Intelligence Information Report (IIR) and stated: "If this needs to get to the military, WFO might have to do it internally."

In conducting its assessment of Hasan, WFO decided not to contact his chain of command. WFO's assessment, although "slim" in San Diego's estimation, concluded that Hasan was not involved in terrorist activities.

Under these circumstances, and in the absence of a formal policy requiring San Diego, WFO, or ITOS 1 to advise DoD about a counterterrorism assessment of a U.S. soldier, the failure of either JTTF to advise DoD about the information or the assessment was not unreasonable. However, the absence of a formal policy on notifying DoD of assessments or investigations of its personnel was unreasonable.

2. The Decision Not to Issue an Intelligence Information Report (Chapter 6)

The FBI did not issue an IIR to DoD and other USIC members concerning Hasan's first two messages. Dissemination of this information would have been appropriate, lawful, and consistent with FBI guidelines.

SD-Agent, SD-Analyst, and SD-TFO2 discussed issuing an IIR about the messages. There was an arguable reason to believe that the messages were foreign intelligence information that could be lawfully disseminated outside the FBI. The first message suggested that a U.S. soldier was seeking Aulaqi's advice on committing violence against fellow soldiers. Given Aulaqi's prominent inspirational role, this information reasonably appears necessary to the ability of the U.S. to protect against international terrorism – in this case, to protect against a U.S. soldier committing acts of violence against fellow soldiers on the battlefield. See 50 U.S.C. § 1801(e).

FBI policy is to share FBI intelligence when dissemination has the potential to protect the U.S. against threats to national security or improve the effectiveness of law enforcement. FBI INTELLIGENCE POLICY MANUAL § 1.7. As noted in Chapter 6, San Diego believed dissemination was permissible if a message reasonably appeared to concern taking part in jihad, engaging in violent conduct, or committing crimes – or if the information was believed valuable to the greater intelligence community. Given Hasan's apparent identity as a U.S. Army officer, his messages met these standards.

San Diego did not issue an IIR because of a mistake in interpreting Hasan's Defense Employee Interactive Data System (DEIDS) record. SD-TFO3 read the abbreviation "Comm Officer" to mean "Communications Officer" rather than "Commissioned Officer." SD-Agent thus believed that Hasan might have access to IIRs. To protect the [redacted] Aulaqi investigation [redacted], he decided not to issue an IIR and noted his concern about issuing an IIR in an email transmitting the lead to San Diego's overseers at FBI Headquarters, ITOS 1, CONUS 6.

SD-TFO3's misinterpretation of the DEIDS record was understandable; indeed, WFO-TFO noted that he had seen others make the same mistake. The mistake had serious consequences, however, because IIRs are a primary means by which the FBI shares information. An IIR could have provided notice to senior DoD officials of Hasan's communication with Aulaqi.

WFO's response to the lead corrected this mistake and identified Hasan as a U.S. Army Major and physician based at Walter Reed Army Medical Center. San Diego's initial interest in sending an IIR was to identify Hasan. 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.

Chapter 9

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, on the other hand, acted as if San Diego had responsibility for Hasan. The confusion resulted from the nature of Discretionary Action leads, as well as a lack of written 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 (Chapter 6)

No FBI written policy establishes ownership of interoffice leads. The FBI practice, however, is that the receiving office owns the lead. That office is responsible for taking action in response to the lead and determining what, if any, additional investigative steps are warranted. No policy or practice distinguishes "trip wire" and other "standalone" leads from other leads for purposes of ownership.

Effective April 2006, San Diego was the Office of Origin for the Aulaqi investigation. San Diego was thus the FBI Field Office with ultimate responsibility for that investigation. As a matter of practice, but not written policy, WFO owned the Hasan lead and had ultimate responsibility for its outcome. However, the lack of clear policy guidance resulted in neither JTTF taking effective ownership of the lead.

B. The Lead (Chapter 6)

San Diego's quarry was a known inspiration for violent extremists. SD-Agent and SD-Analyst believed he had [ambitions beyond radicalization] [redacted]. [redacted] [Their] primary purpose was to use [redacted] [the investigation] to gather and, when appropriate, disseminate intelligence about Aulaqi [redacted]. The "trip wire" effect of [redacted] [the investigation in identifying other persons of potential interest] was, in SD-Agent's words, a "fringe benefit." Certainly it was not the purpose or focus of the [redacted] investigation.

Upon reading Hasan's December 17, 2008, message to Aulaqi, SD-Agent and SD-Analyst identified a potential threat. Hasan asked Aulaqi whether a Muslim in the U.S. military would be considered a martyr for committing violent acts against fellow soldiers. SD-Agent's initial instinct was to determine whether the sender was a U.S. soldier. SD-TFO3 identified a U.S. Army officer named Nidal Malik Hasan who worked at Walter Reed Army Medical Center in Washington, D.C. SD-Agent set a lead to WFO because Hasan worked in its Area of

Responsibility. Before setting the lead, he checked DWS to determine if Aulaqi had responded to the email. He found a second email from Hasan expressing sympathy for the Iranian government.

SD-Agent set a Routine Discretionary Action Lead to WFO that contained both 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 San Diego to set the lead in the ordinary course of business – and thus, as a Routine lead. See MIOG Part II, § 16-1.4(2). Because conventional practice was to give the receiving office discretion in handling assessments of potential threats in its Area of Responsibility, the lead was "[f]or action as deemed appropriate." SD-Agent had set prior leads on other "trip wire" contacts with Aulaqi. Each had been a Routine Discretionary Action lead.

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

San Diego's EC also set an Information Only lead to ITOS 1, CONUS 6 at FBI Headquarters. SD-Agent's cover email stated, in part: "If this needs to get to the military, WFO might have to do it internally." This message indicates SD-Agent's belief that, if WFO established that a U.S. Army officer sent the messages, WFO was responsible for notifying DoD about any assessment or investigation of Hasan. It also underscores San Diego's belief that WFO was responsible for Hasan.

After setting the Hasan lead, SD-Agent and SD-Analyst returned their attention to the Aulaqi investigation. Hasan had no apparent connection to Aulaqi. He had contacted Aulaqi through his website, which suggested that he was a stranger. Nothing in his first two messages suggested an association with Aulaqi. Aulaqi had not responded to him. Because the Hasan lead had no direct relationship to the Aulaqi investigation – which did not need and was not waiting on its results – San Diego believed that Hasan was WFO's responsibility. As a result, SD-Agent and SD-Analyst did not record Hasan's name or email address for future reference. Without a DWS-EDMS [redacted] tool to assist them in tracking [redacted] [and correlating certain email data or to link a new message with earlier messages,] they reviewed sixteen further Hasan-Aulaqi messages over the next five months without tying them to the lead.

C. The Response (Chapter 6)

San Diego knew little about Nidal Hasan, but the available information suggested that a U.S. Army officer sympathetic to the Iranian government might be communicating with an Islamic extremist and radicalizer about violence against fellow soldiers. This potential threat deserved reasonably prompt action.

San Diego set the lead on January 7, 2009. SD-Agent believed that WFO, the receiving Field Office, would assign leads within 48 hours of receipt. FBI written policy requires Immediate and Priority leads to be assigned and resolved within two and twenty-four hours, respectively. See MIOG Part II, § 16-1.4(2). There is no formal policy guidance on the assignment or resolution of Routine leads. The timing of assignments thus depends on the

personal practice of the receiving supervisor. That timing, in turn, is audited at the Field Office/JTTF level. In contrast, FBI written policy directs supervisors to assign assessments generated on the Guardian Threat Tracking System within five business days of the receipt of the Guardian incident. A Headquarters unit, the Assessment Response Team, audits compliance with the Guardian policy.

At WFO, WFO-SSA did not read and assign the lead until February 25, 2009, nearly fifty days after the lead was set. The lead arrived when WFO was dealing with threats involving President Obama's inauguration. That does not excuse a failure to take the simple step of reading and assigning a lead within a reasonable number of days after its receipt.

There is no formal FBI policy that sets a deadline for the completion of work on Routine leads. Because file reviews occur on a quarterly basis, informal FBI policy requires personnel to complete work on Routine leads within ninety days of assignment. In the context of Guardian-based assessments, on the other hand, FBI written policy provides that "[e]very attempt must be made to 'mitigate' Guardian incidents within the first 30 days." [redacted] [FBI policy number redacted]. An extension of this 30-day deadline is permitted only with the written justification of a supervisor.

After WFO-SSA assigned the lead, WFO-TFO waited ninety days – until the day his work on the lead was supposed to be completed – to read it and take action. WFO-TFO could not recall why the work was put off until the ninetieth day. The timing could be coincidental. We believe, however, that 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 in WFO's response pushed Hasan further from the minds of SD-Agent and SD-Analyst, and may have contributed to their failure to connect other Hasan-Aulaqi communications with the lead.

D. <u>The Impasse</u> (Chapter 6)

WFO had an obligation to assist San Diego in the Aulaqi investigation. WFO also had an obligation to determine the importance of the lead to its Area of Responsibility. WFO lacked policy guidance, however, on which office had ultimate responsibility for the lead.

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 WFO's assessment as "look[ing] a little slim" given "limited probing into [Hasan's] background, no contact [with] command, and no interview of [Hasan]." This message indicated that San Diego expected, at the least, that WFO would contact Hasan's command and interview Hasan. WFO did not take those steps and instead offered to "re-assess" if San Diego "request[ed] any specific action."

If SD-TFO3's recollection is accurate, his final phone call with WFO-TFO reflected the failure of either JTTF to take ownership of the Hasan threat. Without clear policy direction, each

looked to the other as responsible and as the final decision-maker. As a result, nothing further was done.

E. Deference to Military Task Force Officers (Chapter 6)

Both Field Offices compounded the lack of ownership by deferring to military TFOs.

SD-Agent asked DCIS and NCIS TFOs in San Diego to determine whether Hasan was a member of the U.S. military. He also involved those TFOs in the decision about whether to circulate an IIR on Hasan. Those actions were reasonable and prudent. Interagency synergy is a prime reason for the JTTF Program.

That synergy weakens, however, when the result is that 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 FBI Agents and Analysts. 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. In this case, 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 appears to have driven the decision not to interview Hasan or contact his superiors.

F. An Inverted Chain of Command (Chapter 6)

The JTTF synergy also weakens when the FBI looks to military TFOs – or those of any other agency – to resolve disputes between JTTFs. Here, after SD-Agent reviewed WFO's response to the lead, he was reluctant to push back. He knew WFO-SSA. They were peers. Yet SD-Agent asked SD-TFO3 to contact WFO-TFO, DCIS Agent to DCIS Agent, even though the two had never met.

SD-Agent took this approach to avoid being, in his words, "the heavy" in dealing with a DCIS Agent in another JTTF. He was also concerned about professional courtesy and deference to another Field Office; indeed, he had pushed back at the response of another Field Office only once before in his career. SD-Agent's request also could have been based in part on SD-TFO3's reaction to WFO's response, which caused SD-TFO3 to wonder whether Hasan was a WFO asset.

SD-Agent's request also underscores the perception of the Hasan assessment as a military matter. That perception led both JTTFs to push the dispute down the FBI chain of command, to be resolved by DCIS TFOs, rather than up the chain of command to FBI supervisors or Headquarters. That action led, in turn, to a lack of resolution – and a lack of further investigation.

We understand SD-Agent's interest in extending professional courtesy and investigative deference to another Field Office. We appreciate the discomfort in challenging a TFO assigned to another Field Office about the sufficiency of his level of investigation. But too much is at stake for these concerns to guide (or deter) resolution of interoffice investigative disputes.

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 routinely handles interoffice disputes and disagreements, but only as a matter of unofficial policy.

G. The Lack of Formal Policies (Chapter 6)

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.

The nature of Routine Discretionary Action Leads only added to the dissonance. At that time, written FBI policy on Discretionary Action Leads placed responsibility on the issuing office to set the lead while apparently placing responsibility on the receiving office to determine the adequacy of any action taken on the lead: "the recipient will decide what, if any, action to take...." MAOP § 10.2.9(1)(b).

The FBI should have provided formal policy guidance on the ownership of leads and interoffice dispute resolution.

Chapter 10

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 DWS-EDMS after the passage of five months, 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 leads and establishing a baseline for information to be collected in 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 (Chapter 6)

WFO-SSA and WFO-TFO assessed Hasan using the limited U.S. 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 also showed that he 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. The two messages in San Diego's lead solicit Islamic opinions. Hasan made no attempt to disguise his identity and used an email address that revealed his proper name. If these two messages and the Electronic Personnel File were the universe of available information, they might provide a reasonable basis to believe that inquiries to a radical Islamic cleric were relevant to Hasan's research.

The U.S. Army records available to WFO-TFO did not present a complete or accurate picture of Hasan. Indeed, their contents were misleading. WFO-TFO did not have access to files maintained locally by Army command. As a result, he was unaware of the Army's issues with Hasan. We believe that DoD should examine whether DoD participants in the JTTF program should have full access to all DoD personnel records.

Despite the Army's interest in Hasan's research, his communications with an inspirational and potentially operational [redacted] [known radicalizer] under FBI investigation deserved scrutiny beyond a simple records check. As the final sentences of San Diego's lead state: "[redacted] Although the content of these messages was not overtly nefarious, this type of contact with Aulaqi would be of concern if the writer is actually the [active duty military officer] identified above." Regardless of his Electronic Personnel File, the lead warranted a closer look at Hasan, even if an interview were ruled out.

B. The Decision Not To Interview Hasan (Chapter 6)

The decision not to interview Hasan was flawed. WFO-TFO and WFO-SSA offered two explanations for it. First, both men believed that an interview could jeopardize the Aulaqi [investigation] [redacted] by revealing the FBI's access to Hasan's messages. This explanation is not persuasive. Pretext interviews are common FBI tradecraft. FBI Agents talk to subjects and assess threat levels every day without explaining the source of their knowledge. Pretexts for interviewing Hasan come easily to mind; for example, an Agent could have approached Hasan to ask for insights into Islamic radicalization, for information about the tolerance of Muslim soldiers in the U.S. military, or to discuss a possible guest lecture by Hasan based on his research.

Second, WFO-TFO and WFO-SSA 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, which in this instance they determined would be contrary to the DIOG's "least intrusive means" requirement. That requirement is straightforward: 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. DIOG § 4.4(B). Thus, when certain information can be obtained from public sources, Agents and TFOs generally should not obtain that information through more intrusive means, such as physical surveillance.

Here, San Diego's lead advised that, "[w]hile e-mail contact with Aulaqi does not necessarily indicate participation in terrorist-related matters ... this type of contact with Aulaqi would be of concern if the writer is actually the individual identified above." In response to the lead, WFO conducted an assessment to determine whether Hasan was "involved in terrorist activities." The first and only method WFO used to secure that knowledge was a records check. The available files suggested that Hasan's messages involved research, not terrorism; but 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. This is how the least intrusive means requirement is supposed to operate: selecting, step-by-step, the least intrusive technique(s) that will accomplish the operational objective at hand.

SD-TFO3's recollection of his final telephone call with WFO-TFO, if correct, indicates that another factor played a role in WFO's decision not to interview Hasan. According to SD-TFO3, he called WFO-TFO on or about June 15, 2009, and told him that, upon receiving a lead like this one, San Diego would have conducted, at the least, an interview of the subject. SD-TFO3 recalls that WFO-TFO replied, in effect (paraphrased, not a quotation): "This is not SD, it's DC and WFO doesn't go out and interview every Muslim guy who visits extremist websites."

According to SD-TFO3, WFO-TFO also advised him that this subject is "politically sensitive for WFO."

C. The Failure To Search For Additional Messages (Chapters 4 and 6)

Hasan sent his first two messages on December 17, 2008, and January 1, 2009. San Diego set the lead on January 7, 2009. Before setting the lead, SD-Agent searched DWS to determine whether Aulaqi had responded to Hasan's first message. That search returned Hasan's second message.

In reviewing the lead and making the assessment five months later, neither WFO-TFO nor WFO-SSA considered searching DWS-EDMS to determine if Aulaqi had responded to these messages – or, indeed, if there were additional messages. Likewise, after reviewing WFO's assessment of Hasan, neither SD-Agent nor SD-Analyst considered searching DWS-EDMS to identify "additional information" that might cause WFO to "re-assess this matter."

The failure to search for additional messages resulted primarily from the FBI's failure to provide TFOs with training on and access to DWS-EDMS and other FBI databases, the search and information management limitations of DWS-EDMS, the lack of ownership of the Hasan lead, and the absence of the type of initiative that Agents, Analysts, and TFOs should be encouraged to take, particularly when confronted with dissonant information or an interoffice dispute.

The FBI's failure to instruct TFOs on the existence and use of DWS-EDMS – and to provide them with training on and access to the system – was unreasonable. The two TFOs primarily involved in the Hasan assessment – WFO-TFO and SD-TFO3 – did not even know that DWS-EDMS existed until after the Fort Hood shootings. Although SD-TFO1 and SD-TFO2 knew about DWS-EDMS – and SD-TFO2 received training on the system in April 2009 – neither of them had access to the system until after the shootings.

Because of WFO-TFO's lack of knowledge, neither he nor anyone else at WFO searched DWS-EDMS using Hasan's name or email address. WFO-TFO did search the FBI's Telephone Applications using the telephone number in Hasan's DEIDS record. He also searched ACS using Hasan's email address, assuming incorrectly that San Diego would place any additional messages of note into that system. After finding only the lead, WFO-TFO made no further inquiries or searches of FBI databases. He did not ask his squad's IA for assistance. He did not search the Investigative Data Warehouse (IDW) or the Data Loading and Analysis System (DaLAS), the FBI's two largest databases of investigative and intelligence information. His limited searches and mistaken assumption about ACS reveal a broader lack of training on the FBI's most precious counterterrorism resource – its information.

When presented with WFO-TFO's analysis and conclusions, WFO-SSA did not think to ask whether Aulaqi had responded to Hasan's messages or whether there had been additional messages during the five-month interlude. He did ask whether WFO-TFO had searched FBI databases. WFO-TFO's affirmative response could have caused WFO-SSA to believe that he had searched DWS-EDMS, IDW, and DaLAS.

The failure to search DWS-EDMS and WFO-SSA's failure to confirm which databases had been searched, appear to have had significant ramifications. Depending on the search technique, that search, if performed on May 25, 2009, could have returned as many as [redacted] additional messages from Hasan, as well as Aulaqi's two emails to Hasan. The additional messages could have undermined the assumption that Hasan had contacted Aulaqi simply to research Islam. Indeed, WFO-SSA said – with the benefit of hindsight – that WFO would have opened a preliminary investigation of Hasan if he had seen all of the additional messages.

After receiving WFO's response, San Diego failed to search DWS-EDMS to determine whether there had been additional communications during the intervening five months. Under the circumstances, that failure is not unreasonable. SD-Agent and SD-Analyst believed that WFO had reviewed DWS-EDMS as part of the Hasan assessment. WFO's response to the lead stated that "WFO reviewed FBI and Department of Defense databases and record systems" and referred to Hasan's "to date unanswered email messages," which implied that WFO had reviewed DWS-EDMS. Moreover, SD-Agent and SD-Analyst had been reviewing the [information acquired in the Aulaqi investigation] [redacted] throughout the intervening five months, and no doubt believed – although perhaps mistakenly – that they would have identified any other messages of interest.

The collective failure of WFO and San Diego to review DWS-EDMS in May and June 2009 also underscores the lack of clear policy guidance on which Field Office owned the Hasan lead. WFO believed that it was San Diego's responsibility to forward any additional messages of interest that were relevant to the lead. San Diego, on the other hand, believed that it was WFO's responsibility to search DWS-EDMS and other FBI databases when acting on the lead.

D. WFO's Baseline Collection for Assessment (Chapter 6)

On September 24, 2009, the FBI Counterterrorism Division sent an Electronic Communication (EC) to all Field Offices with guidance on the Division's "Baseline Collection Plan" for terrorism assessments and investigations. FBI Counterterrorism Division, *Baseline Collection Plan Administrative and Operational Guidance* (Sept. 24, 2009). Baseline Collection is a framework, consistent with the DIOG, "to guide investigators in obtaining information and intelligence and using investigative methods during the course of each DT [Domestic Terrorism] and IT [International Terrorism] investigation." The Division intended the Baseline Collection "to establish a foundation of intelligence upon which the FBI may base the decision to continue or close an assessment or investigation."

The EC identifies a series of actions that constitute the expected Baseline Collection of information when conducting an assessment or investigation. Although not sent until September 2009, the EC represents a relatively contemporaneous objective standard for measuring the reasonableness and adequacy of WFO's assessment of Hasan and San Diego's view of that assessment. (Because the EC was effective on November 15, 2009, and thus parallels in time the FBI's remedial responses to the Fort Hood shootings, we examine its sufficiency in Part Three.)

The Baseline Collection standards include the following questions and searches relevant to the Hasan assessment:

> Is there reason to believe that your subject has been in email contact with subjects of other FBI investigations? If so, compare relevant data concerning the subject's email account(s) contained within FBI databases: DWS/EDMS, ACS, IDW and DaLas.
>
> Is there reason to believe that the subject has purchased or is licensed to possess firearms or explosives? If so, run NCIC checks and/or contact local ATF representatives or any available State database in the relevant jurisdiction to collect responsive records or information.
>
> Is there any reason to believe, considering the subject's background, including employment and criminal history, that he has received specialized training or experience or has specialized knowledge in military tactics or operations, law enforcement, firearms or explosives, or similar subjects?

Viewed under the Baseline Collection standards, WFO's assessment was deficient in failing to search for "relevant data concerning the subject's email account(s) contained within FBI databases" including DWS-EDMS. That search, if conducted on May 25, 2009, would have disclosed (depending on the search technique) as many as [redacted] additional messages from Hasan to Aulaqi, as well as Aulaqi's two emails to Hasan. WFO's assessment also did not pursue the questions concerning firearms ownership and training, experience, and knowledge in military tactics; but the revelation that Hasan was a U.S. Army psychiatrist may have tempered any concern about these subjects.

The Baseline Collection standards do not require interviews as part of an assessment. Instead, after the Baseline Collection is obtained, the "Assessment may continue until factual information is developed that warrants opening a predicated investigation or until a judgment can be made that the target does not pose a terrorism or criminal threat." The EC thus supports the reasonableness of San Diego's view that the assessment was inadequate. It also supports the reasonableness of San Diego's belief that, at minimum, WFO would have reviewed DWS-EDMS as part of the Hasan assessment.

E. Workload and the Lack of Formal Policies (Chapter 6)

We cannot assess the role that workload played in the assessment. 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 CT-1 was overburdened. If so, that underscores the importance of formal policy direction that allows supervisors as well as SAs, IAs, and TFOs to understand, prioritize, and manage their workloads. Otherwise, the FBI risks creating circumstances in which Routine leads are prioritized by the order of receipt, rather than the order of potential importance

Formal deadlines would have required WFO-SSA and WFO-TFO to read the Hasan lead at earlier dates and make informed decisions about whether to assign and complete the lead at earlier dates.

Likewise, a formal policy on baseline collections for assessments like the one instituted on September 24, 2009, would have advised WFO-TFO about the existence of DWS-EDMS and caused WFO to search [information acquired in the Aulaqi investigation] [redacted]. That search, if performed on May 25, 2009, could have located as many as [redacted] additional messages from Hasan, as well as Aulaqi's two emails to Hasan.

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

Chapter 11

Information Technology and Information Review Workflow

A. Information Technology Limitations (Chapter 4)

STAS designed DWS in 2001 as a transactional database to record [redacted] [all communications] intercepts [redacted]. In the intervening years, DWS-EDMS has been transformed into a warehouse database that holds [redacted] information obtained [through exercise of the FBI's criminal and counterterrorism authorities (see Chapter 3).] [redacted]. Through a series of STAS improvements and enhancements beginning in 2009 and continuing today, DWS-EDMS is a capable tool for the review of the ever-increasing [redacted] [volume of investigative] information, but it lacks the modern hardware infrastructure needed to fulfill and preserve its crucial functionality.

The lack of a modern hardware infrastructure has two major implications. First, the relatively aged server configuration for DWS-EDMS and its ever-increasing data storage demands, coupled with ever-increasing use, creates slowdowns that we witnessed repeatedly in our hands-on use of the system. An Agent in the field with considerable DWS-EDMS experience reported that the slowdowns deterred searching the system.

Second, DWS-EDMS lacks a "live" or "failover" disaster recovery backup. [redacted]

B. Information Review Workflow (Chapters 4 and 5)

In examining San Diego's [redacted] review of the [information acquired in the Aulaqi investigation] [redacted], we identified serious concerns about the available technology and two interrelated concerns about human actions: questionable decisions in [redacted] [reviewing] certain Hasan-Aulaqi communications and the failure to relate later communications to the lead set on January 7, 2009. Our investigation of these matters leads us to conclude that the technological tools and review workflow for this [information] [redacted] were inadequate.

With the admitted benefit of hindsight – and a lack of broader context – we may disagree with certain decisions SD-Agent and SD-Analyst made when reviewing [redacted] the Hasan-Aulaqi communications. For example, between February 2 and March 3, 2009, Hasan sent

several messages to Aulaqi offering financial assistance. These messages triggered Aulaqi's only two responses. On May 31, 2009, Hasan suggested that he viewed suicide bombing as permissible in certain circumstances. SD-Agent [redacted] [identified] each email as "Non-Pertinent" and "Not a Product of Interest." He explained the financial-assistance messages as relating only to the upkeep of Aulaqi's website. He dismissed the suicide-bombing message because Hasan seemed to describe a third-party's opinion, although Hasan wrote that the logic "make[s] sense to me" and that "I would assume that [a] suicide bomber whose aim is to kill enemy soldiers or their helpers but also kill innocents in the process is acceptable."

We are mindful that SD-Agent is the Case Agent on the Aulaqi investigation and that the words of Aulaqi and his associates were the focus as SD-Agent and SD-Analyst reviewed the [information] [redacted]. We are unable to assess the reasonableness of these [redacted] [identifying] decisions outside the context of the [redacted] [nearly 20,000] other Aulaqi-related [redacted] [electronic documents] that SD-Agent and SD-Analyst reviewed [redacted] in the sixteen months between March 16, 2008, and June 17, 2009.

We find, however, that the FBI's information technology and document review workflow did not assure that all [redacted] [information] would be identified [redacted] 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 [redacted] [volume of the Aulaqi information] [redacted]; (4) the workload; (5) limited training on 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] [redacted].

C. <u>The Human Factor</u> (Chapters 4 and 6)

Agents, Analysts, and Task Force Officers are human. We may hope for, but we cannot expect, perfection. [redacted] [FBI governing authorities] require reviewers to decide whether a document is "Not Pertinent" or "Pertinent." (Like reviewers in the field, we use "Pertinent" to describe the categories of information that fulfill the [requirements] [redacted]. Research shows that trained information reviewers faced with binary decisions like those made by [redacted] [FBI] reviewers – relevant/irrelevant, responsive/non-responsive, pertinent/non-pertinent – identify only about 75% of the relevant documents and, indeed, agree with each other's decisions only about 75% of the time (<u>see</u> Chapter 4).

Although differences in the background and experience of reviewers, as well as extrinsic and random factors (for example, inattention, distraction, fatigue, or illness) can produce variations in accurate decision-making about the relevance – or, in the review of [redacted] [case information], pertinence – of information, the primary factors are those we now discuss.

D. **The Language Barrier (Chapters 4 and 6)**

[redacted]–The inherent ambiguity of language and the presence of jargon, idiom, foreign languages, and code challenge even the most capable reviewers and search technologies.

E. **The Data Explosion (Chapters 4 and 6)**

The exponential growth in the amount of electronically stored information is a critical challenge to the FBI. As of May 2011, the holdings of DWS-EDMS exceeded [redacted] of data, the equivalent of [redacted] printed pages of text. DWS-EDMS holdings increase, on average, by [redacted] files each week.

[redacted]

F. **Workload (Chapters 4, 5, and 6)**

The Aulaqi [investigation] [redacted] is a stark example of the impact of the data explosion. SD-Agent and SD-Analyst confronted a weighty review task [redacted]. SD-Agent spent approximately three hours each day reviewing the [redacted] [information acquired in the Aulaqi investigation]. SD-Analyst spent about 40% of his time on the investigation.

By November 5, 2009, the date of the Fort Hood shootings, the Aulaqi [investigation] [redacted] had required SD-Agent and SD-Analyst to review 29,041 [redacted] [electronic documents – on average,] approximately 1,525 [redacted] per month, or 70 to 75 [redacted] per work day. At times, the average number of [redacted] [electronic documents reviewed] ranged higher than 130 per work day.

The complexity of their review task was exacerbated by [the diversity of the electronic information]. [redacted]

As these statistics show, the [redacted] [information review demands of the Aulaqi investigation were] relentless. The constant flow of [redacted] [information] and the nature of the Aulaqi threat required SD-Agent and SD-Analyst to [devote time throughout each day to its review]. [redacted]

G. [Identifying] Requirements (Chapters 4, 5, and 6)

FBI policies required SD-Agent and SD-Analyst to make [multiple] decisions about each product, [including] Attorney-Client Privilege, Workflow, and Translation. Although the categories include an Unreviewed/ Undecided checkbox, the FBI trains and expects reviewers to make [identification] decisions immediately upon reviewing each product.

H. The Lack of DWS-EDMS Training (Chapters 4, 5, and 6)

To obtain DWS-EDMS access, an Agent, Analyst, or TFO must first complete three training courses in the FBI's Virtual Academy. None of these courses provides instruction on how to use the DWS-EDMS search tool or other functionalities.

Many Agents and most TFOs did not receive training on DWS-EDMS and other FBI databases until after the FBI's internal investigation of the Fort Hood shootings. Even for Agents and Analysts with access before the Fort Hood shootings, there was no formal training program for DWS-EDMS; instead, most "training" was on the job. Our interviews and visits to the field revealed significant disparities in skill at using the search and management functions of DWS-EDMS.

I. Search Tools (Chapters 4 and 6)

Although not originally designed as a warehouse database, DWS-EDMS became the depository of information [acquired through the exercise of its criminal and counterterrorism authorities and techniques]. Today, DWS-EDMS is a capable, if overburdened, tool for the conventional review of [information] and has improved dramatically with its [September 2011] incarnation. In early 2009, however, DWS-EDMS lacked functionalities for the effective review and management of [the large quantities of information collected in the Aulaqi investigation]. Even today, it lacks the modern hardware needed to fulfill its potential.

Our interviews with DWS-EDMS users, including the participants in the Hasan matter, elicited the following typical comments about the system: "awkward"; "complex"; "difficult"; "cumbersome"; and "terrible." Each user, not unexpectedly, had particular issues with the system's search tools, management tools, and responsiveness.

We replicated, through hands-on use of the technology, the steps taken by SD-Agent and SD-Analyst in reviewing the [information acquired in the Aulaqi investigation] and, in particular, the Hasan-Aulaqi communications. We undertook searches of DWS-EDMS using Hasan's name and email address that could have been pursued by WFO and San Diego in 2009. We also performed or supervised other searches of DWS-EDMS to test its

functionality. Our hands-on experience with the system confirms the assessments of users in the field.

1. Two Interfaces

In May 2009, the Special Technology Applications Section (STAS) upgraded the DWS-EDMS graphic user interface (GUI) to reduce the number of menus and commands, reorganize filters and preferences, and provide three new search methods (by case ID, court-assigned docket number, and facility). However, STAS retained the original GUI – now called DWS-EDMS Classic – as an alternative interface because the new GUI lacked its analysis tools and report capabilities. As a result, users must choose which GUI to use in reviewing [redacted] [acquired communications products]. Each has advantages and disadvantages. As noted below, the choice may affect the outcome of searches.

2. Search Limitations

DWS-EDMS search capabilities are limited. The primary search modes are by [redacted]. These searches are literal, and return only documents containing the specified identifier or keyword, whether alone or in specified relationships (a "Boolean" search – for example, ("smoking" and "gun") or ("smoking" within five words of "gun"). Anyone who has used Westlaw, Lexis, or Google understands the methodology. Relying on keyword searches to identify, compare, analyze, tag, and retrieve information of potential interest is time-consuming, impractical, and inefficient. It is also risky.

Keyword searches are both under- and over-inclusive. They return only those electronic records containing the specified word or words, and will not capture documents using similar words – for example, abbreviations, acronyms, synonyms, nicknames, and misspellings. Thus, a search for "gun" will not return "pistol" or "rifle." At the same time, keyword searches capture every document, whether potentially relevant or not, that contains a keyword; thus, a search for "gun" will return documents involving a squirt gun, a glue gun, the phrase "under the gun."

Increasing the number of keywords may reduce the risk of missing responsive information. A dedicated search for "gun" should include synonyms like "pistol" and "rifle" and "weapon"; but the greater the number of keywords, the greater the number of non-responsive records that will be returned.

The search technique may also affect the outcome. We found, for example, that a "full text" search for products containing the email address NidalHasan@aol.com returned only nine of the eighteen Hasan-Aulaqi communications, even though that address appeared in every one of them. The reason is that a DWS-EDMS full text search will not return [redacted]. A "participant" search, on the other hand, returned all of the communications. We learned of similar experiences during our interviews. For example, WFO-TFO reported that, in the aftermath of the shootings, WFO-Analyst searched Hasan's email address in DWS-EDMS and obtained different results depending on whether she used DWS-EDMS or DWS-EDMS Classic.

3. Potential Inaccuracy

[I]ssues with the search index used on DWS-EDMS create the possibility that full text searches of the system will be incomplete.

4. Responsiveness

The hardware hosting DWS-EDMS [is dated] . It is operating under maximum stress. As a result, the responsiveness of the DWS-EDMS database to search queries is remarkably slow. Our test searches produced wait times for results that took twenty seconds and longer, and occasionally "timed out" (i.e., failed because of the time consumed by the search). One Agent noted that, with a [long] wait for the system to open a new window, DWS-EDMS deterred searches.

J. Management Tools (Chapters 4 and 6)

When San Diego set the Hasan lead in January 2009, DWS had no tool for [automatically tracking and correlating certain email data] . Although the DWS-EDMS upgrade in February 2009 eliminated certain of these shortcomings, those fixes came long after San Diego set the lead.

Because of these shortcomings, SD-Agent and SD-Analyst had to [correlate email data] outside DWS . SD-Agent used his memory and notes. SD-Analyst used an Excel spreadsheet and notes. Because Hasan was a "trip wire" lead and not apparently relevant to the Aulaqi investigation – and underscoring the lack of policy guidance on ownership of the lead – neither [SD-Agent nor SD-Analyst] recorded Hasan's name or email address for potential future reference.

Requiring reviewers to rely on memory, off-system records, or a manual search process to [correlate email data] is not feasible in a data-heavy working environment. Indeed, as the Hasan matter reveals, it may be risky.

K. Lack of Managed Document Review and Quality Control (Chapters 4, 5, and 6)

Because any review of information is prone to error, the standard for information review is not perfection, but accuracy within tolerances that are consistent with professionalism, diligence, and reasonable care. These tolerances require well-designed quality control measures based on effective training, project management, performance measurement, and reporting. The FBI did not provide the San Diego reviewers with any of these basic safeguards.

SD-Agent and SD-Analyst were the only two FBI personnel [redacted] [reviewing] the communications [acquired in the investigation] of the leading English-speaking inspiration for violent Islamic extremism. Their ideal, not always fulfilled, was that both of them would review all new products over the course of each work day. There was no other backstop. Although International Terrorism Operations Section (ITOS) 1, Continental United States (CONUS) 6 had program management responsibility for overseeing the San Diego JTTF's intelligence collection and investigative efforts, the FBI had not implemented any procedures for ITOS 1, CONUS 6 to assess, validate, or contextualize the results of San Diego's review, whether to detect potential [redacted] [identification] errors, identify information requiring additional review, link disparate message threads, assess the potential for additional "trip wire" investigations, or conduct retrospective strategic analysis.

L. The Workflow (Chapters 4, 5, and 6)

The confluence of these diverse human and technological factors forced SD-Agent and SD-Analyst to review, [redacted] using a linear, forward-looking workflow, [redacted] each of the Hasan-Aulaqi communications [redacted] in isolation as eighteen of the nearly 8,000 [redacted] [electronic documents] [redacted] that they reviewed between December 18, 2008, and June 16, 2009. That workflow encouraged anticipatory review, analysis, and [redacted] identification of [redacted] 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.

The decision on [redacted] [information's] "Pertinence" depends primarily on the [redacted] [content] of the [redacted] [information]; its context; the reviewer's knowledge of the subject matter, the sender, and/or the recipient; the reviewer's training and experience – and ideally, on a broader perspective drawn from other [information in the investigation] [redacted], intelligence located elsewhere in the FBI's possession, and other reviewers. As SD-Agent learned when he searched DWS-EDMS before setting the Hasan lead, the decision also depends on time. That search located a second Hasan message to Aulaqi, which SD-Agent had reviewed only days earlier and [redacted] [identified] "Not a Product of Interest." Read later and in the context of the first message, the second message became part of an EC setting a lead on a potential terrorism threat.

Decisions on pertinence may be tactical (the Hasan lead) and strategic (the Aulaqi investigation). Agents, Analysts, and Task Force Officers may have different goals in mind when assessing electronic information and these goals may vary over time. The limited search and management capabilities of DWS-EDMS as it existed in 2008-2009 and a linear, forward-looking, unmanaged workflow prevented San Diego from connecting Hasan's messages and making strategic judgments about those messages.

Part Three

Assessment Of FBI Remedial Actions

Following its internal review of the Fort Hood shootings, the FBI made important changes to its policies, operations, and technology. The FBI and the Department of Defense (DoD) recommended certain of these changes to the Assistant to the President for Homeland Security and Counterterrorism on November 30, 2009. In the months that followed – and in the wake of the attempted Christmas Day 2009 bombing of Northwest Flight 253 and the attempted Times Square bombing of May 1, 2010 – further changes have occurred.

The Terms of Reference asked Judge Webster to examine "whether the steps the FBI is taking following an internal review of the shooting are sufficient or whether there are other policy or procedural steps the FBI should consider to improve its ability to detect and deter such threats in the future."

We applaud the steps the FBI took in response to its internal review and subsequent events. In this Chapter, we assess those steps. In Part Four, we discuss additional policy, procedural, and technological improvements that the FBI should consider to improve its ability to detect and deter future threats.

A. Information Sharing

1. FBI-DoD Clearinghouse Process for Counterterrorism Assessments and Investigations of Military Personnel

Effective November 2009, the FBI and DoD adopted a clearinghouse procedure to provide notice to DoD of any FBI counterterrorism assessment or investigation of a known member of the military, a known DoD civilian employee, or a person known to have access to military facilities. Under this procedure, JTTFs must notify the Counterterrorism Division – which, in turn, notifies the NJTTF – upon opening the assessment or investigation. The notification must include the subject's identity and branch affiliation, the basis or predication for the assessment or investigation, and contact information for the FBI case agent and supervisor. However, the notification cannot contain information that cannot be disseminated under FISA Minimization requirements.

The NJTTF must, within ten days, transmit the notification by Letterhead Memorandum (LHM) to the appropriate headquarters Military Counterintelligence Service and to the Deputy Director of the Defense Intelligence Agency's Defense Counterintelligence and HUMINT Center (DCHC). Within ten days of receiving the LHM, those military entities must send a confirmation of receipt to the FBI. This process is designed to provide notice at the executive level and the field level.

The FBI and DoD implemented these procedures informally in late November 2009. The FBI formally implemented the procedures by a memorandum to the field on January 7, 2010.

In late November 2009, the FBI sent DoD a listing of [redacted] active counterterrorism assessments and investigations with a military nexus. By May 2011, the FBI had used this clearinghouse process to notify DoD of an additional [redacted] counterterrorism assessments or investigations of military/DoD personnel.

Conclusion: This procedure assures that, as a matter of written policy, the FBI will provide timely and consistent notice of counterterrorism assessments and investigations of known members of the military, DoD civilian employees, and others with access to military facilities to DoD at the executive and field levels. It is an important information sharing development.

If this procedure had been implemented prior to November 5, 2009, its impact on the Hasan assessment is a matter of conjecture. Although the procedure might have raised the visibility of the assessment inside the FBI, it might not have changed WFO's assessment or San Diego's reaction to that assessment. The primary impact would have depended on DoD's response and any action that DoD investigators would have taken alone or in cooperation with the FBI.

We do not believe that this clearinghouse procedure alone is sufficient to resolve the information sharing issues implicated by this matter. As discussed in Part Five, we recommend that the FBI create a formal policy establishing a clearinghouse procedure for counterterrorism assessments and investigations of known law enforcement personnel. We also recommend that the FBI proceed with plans to identify other federal departments and agencies (for example, the Department of State and the Transportation Security Administration) as potential subjects of comparable information sharing procedures – thus requiring JTTFs to inform the Counterterrorism Division and the NJTTF (and, if appropriate, the relevant department or agency) of counterterrorism assessments and investigations involving employees of those departments and agencies.

2. Consolidation of FBI-DoD Memoranda of Understanding on Information Sharing, Operational Coordination, and Investigative Responsibilities

DOJ and DoD have executed, effective August 2, 2011, a base agreement (MOU) setting forth a framework for future agreements governing information sharing, operational coordination, and investigative responsibilities between the FBI and DoD. Through annexes to the base agreement, the FBI and DoD will define each party's investigative responsibilities, as well as obligations and responsibilities to share information and to coordinate operations.

The FBI and DoD are negotiating subject matter-specific annexes that will govern, among other things, information-sharing and operational coordination/jurisdiction in counterterrorism and counterintelligence contexts and the sharing of the Terrorist Screening Center's watchlist information.

When the annexes on information-sharing and operational coordination/jurisdiction in counterterrorism and counterintelligence contexts are signed, they and the base MOU will collectively supersede the Agreement Governing the Conduct of Department of Defense Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (1979) and its 1996 supplement, as well as the MOU Regarding Coordination of Counterintelligence Matters (1991).

Conclusion: There are approximately 167 FBI-DoD Memoranda of Understanding. Some 114 of these agreements concern, at least in part, information-sharing. (A number of these agreements involve specific operations or situations, and are effectively inoperative.) We believe that the base MOU and its annexes on information-sharing and operational coordination represent a major step toward consolidating and refining those diverse agreements. We encourage the FBI and DoD to continue in their efforts to consolidate and refine those agreements that are fundamental to their shared responsibilities.

B. Operations

1. Discontinuance of "Discretionary Action Leads"

In the relevant time frame, the FBI permitted three types of leads: Action Required, Discretionary Action, and Information Only. MANUAL OF ADMINISTRATIVE OPERATIONS AND PROCEDURES (MAOP) § 10.2.9(1). "Action Required leads are used if the sending office requires the receiving office to take some type of action.... Discretionary Action leads are used if the sending office has some information that may be of importance to the receiving office. These leads may or may not require action by the recipient, and the recipient will decide what, if any, action to take.... Information Only leads are used for information only and when no specific action is required or necessary." MAOP § 10.2.9(1)(a)-(c).

By Electronic Communication (EC) dated March 2, 2010, the FBI discontinued the use of Discretionary Action leads effective March 19, 2010. All pending Discretionary Action leads were to be completed no later than May 20, 2010, or converted into Action Required leads. As a result of this change, any lead issued for other than informational purposes is an Action Required lead. The receiving Field Office cannot ignore the lead, and must do something in response. The EC directs personnel setting Action Required Leads to "adhere to the concept of utilizing the least intrusive alternative that is operationally sound, effective and efficient in obtaining the desired investigative outcome."

Conclusion: The elimination of Discretionary Action leads creates a single category of working leads and avoids prioritization of leads based on the designations Action Required and Discretionary Action. It also assures that receiving Field Offices take some action in response to every working lead.

In setting Action Required leads, however, a Field Office may continue to allow the receiving Field Office to decide what action to take. In other words, the discontinuation of Discretionary Action leads does not necessarily require the sending Field Office to specify actions to be taken or eliminate the receiving Field Office's discretion in deciding what action to take. That is understandable, given the practical need to defer to the receiving office's expertise in its Area of Responsibility, its resources, and potentially greater experience with handling the subject matter of the lead.

If this change had been made prior to the Hasan matter, we believe – and the JTTF personnel involved agree – that it would not have changed San Diego's lead or WFO's response. San Diego would have set an Action Required lead that gave WFO discretion on how to handle

the lead. WFO would have taken the same actions in response to that Action Required lead as they did in response to the Discretionary Action lead.

The elimination of Discretionary Action leads is thus important; but, on its own, it is not a sufficient remedy. Timely and effective action on Action Required leads demands written policies imposing formal deadlines for responding to leads, identifying the minimum information to be gathered in response to leads (consistent with the "least intrusive means" principle), and resolving conflicts between JTTFs and Field Offices about the adequacy of an assessment or investigation. The FBI has taken some, but not all, of the steps necessary to resolve these issues. We recommend that it take the remaining steps (see Part Five).

2. Counterterrorism Baseline Collection Plan

On September 24, 2009, the Counterterrorism Division sent an EC to all Field Offices with guidance on the Division's new "Baseline Collection Plan" for counterterrorism assessments and investigations. FBI Counterterrorism Division, *Baseline Collection Plan Administrative and Operational Guidance* (Sept. 24, 2009). The EC took effect on November 15, 2009, ten days after the Fort Hood shootings. Before that date, the FBI did not prescribe the minimum information that should be collected in counterterrorism assessments and investigations. Although not technically a post-Fort Hood corrective action, we assess the Baseline Collection Plan as a contemporaneous action that is relevant to the discontinuation of discretionary leads and to minimizing the risks of future assessments and investigations.

The Baseline Collection Plan is a framework, consistent with the DIOG, "to guide investigators in obtaining information and intelligence and using investigative methods during the course of each DT [Domestic Terrorism] and IT [International Terrorism] investigation." The Division intended the Plan "to establish a foundation of intelligence upon which the FBI may base the decision to continue or close an assessment or investigation." *Baseline Collection Plan Administrative and Operational Guidance* at 2.

The Plan identifies a series of inquiries and actions that constitute the expected minimum Baseline Collection of information when conducting assessments and investigations. Those actions do not require interviews as part of assessments, but do require a level of inquiry that exceeds the steps taken in the WFO assessment of Hasan.

Conclusion: The Baseline Collection Plan provides useful guidance to Agents, Analysts, and TFOs about the factual information that is basic to most assessments and preliminary investigations. The Plan also standardizes the basic information to be collected. As with any baseline, there is a risk that its minimum requirements could stifle creative thinking and become a checklist – the ceiling, rather than the floor, for information collection. We encourage effective training, communications, and reminders about the Plan to assure that its minimums are perceived as a starting point, not an ending one.

If the Baseline Collection Plan had been implemented prior to the Hasan assessment, its impact on the outcome could have been significant. The Plan states that, if "there [is] reason to believe that your subject has been in email contact with subjects of other FBI investigations," the Agent, Analyst, or TFO must "compare relevant data concerning the subject's email account(s)

contained within FBI databases: DWS/EDMS, ACS, IDW and DaLas." That requirement, if met, would have alerted WFO-TFO to the existence of DWS/EDMS and caused someone at WFO to search that database on his behalf. Depending on when and how that search was conducted, it could have revealed the existence as many as fourteen additional communications between Hasan and Aulaqi. The content of those communications or Hasan's persistence in sending unanswered emails could have changed WFO's assessment of Hasan – or, at least, prompted an interview and discussions with his chain of command. The potential impact on the assessment underscores the importance of effective implementation of the Baseline Collection Plan.

3. [redacted] [Certain Conduct] Triggers Investigation

As a result of the Fort Hood shootings, the FBI opened assessments [of certain U.S. persons] [redacted]

Conclusion: This trigger is appropriate [redacted] post-Fort Hood [redacted], given [Aulaqi's] [redacted] highly publicized reputation in the aftermath of the shootings and the attempted Christmas Day 2009 bombing of Northwest Airlines Flight 253.

Whether [redacted] [this trigger] would have been reasonable before the shootings [redacted] is more problematic. As of November 5, 2009, Aulaqi was the subject of a Tier [redacted] investigation. A considerable [redacted] [amount of information acquired in the Aulaqi investigation] concerned mundane issues [or] [redacted] implicated First Amendment protections. [redacted] [Implementation of this trigger before November 5, 2009], would have been inconsistent with [redacted] civil liberties and privacy interests [redacted].

[The redacted portion involves classified FBI investigative techniques and ongoing investigations.]

4. Decisions to Close Certain Investigations of DoD Personnel

At the time of the Fort Hood shootings, FBI and DoD practice was to elevate any objections by one entity to the other's decision to close an investigation of a military member, civilian DoD employee, or other person with access to military facilities. The FBI and DoD are formalizing this practice in the MOU annex on counterterrorism operational coordination (see Section A.2).

Conclusion: As a result of the implementation of the FBI-DoD Clearinghouse Process for Counterterrorism Assessments and Investigations of Military Personnel (see Section A.1), military investigative agencies should be involved, directly or indirectly, in all FBI investigations

of relevant personnel. By formalizing this pre-existing practice in the MOU annex, FBI and DoD will assure that a consistent conflict resolution process is in place.

5. Identification and Designation of Strategic Collections [redacted]

The FBI Counterterrorism Division and Directorate of Intelligence have designated certain foreign intelligence collections [redacted] as Strategic Collections [redacted]. FBI Headquarters – and, when appropriate, [redacted] [other government agencies] — will [apply additional resources and conduct] [redacted] additional analysis of data collected [redacted] [through] Strategic Collections [redacted]

By definition, the Strategic Collection [redacted] designation will assure that additional review and analysis will apply to any [redacted] [identified connection] between known DoD personnel, law enforcement personnel, security clearance holders, and others with major radicalizing forces.

Conclusion: The Hasan matter shows that certain [redacted] [intelligence collections] [redacted] serve a dual role, providing intelligence on the target while also serving as a means of identifying otherwise unknown persons with potentially radical or violent intent or susceptibilities. The identification and designation of Strategic Collections [redacted] will allow the FBI to focus additional resources – and, when appropriate, those of [redacted] [other government agencies] – on collections most likely to serve as "trip wires." This will, in turn, increase the scrutiny of information that is most likely to implicate persons in the process of violent radicalization – or, indeed, who have radicalized with violent intent. This will also provide Strategic Collections [redacted] with a significant element of program management, managed review, and quality control that was lacking in the pre-Fort Hood [review of information acquired in the Aulaqi investigation] [redacted].

If implemented prior to November 5, 2009, this process would have [redacted] [enhanced] the FBI's ability to [redacted] identify potential subjects for "trip wire" and other "standalone" counterterrorism assessments or investigations. However, its practical impact is uncertain. Given the then-existing limitations on DWS-EDMS search and data management capabilities, Headquarters review might not have provided added value unless managed document review and quality control protocols were in place.

C. Technology

Because of the large and ever-increasing amount of electronically stored information in FBI data stores, any change in policy or procedure that affects the collection, storage, review, search, identification, or management of data must be assessed carefully for its practical impact on human resources and the review workflow.

1. Automatic Linking of Email [Data]

STAS modified DWS-EDMS on February 17, 2010, to inform users [automatically of links between certain email data].

Conclusion: This is a useful, although limited, revision of DWS-EDMS search functionality. The link eliminates the need for reviewers to open a search window. More important, it enables DWS-EDMS users to view [information] in a broader context. The reviewer can thus make better-informed decisions about the [email data].

This revision is a good example of the way in which automation of even relatively simple tasks can expedite, assist, and inform the review of electronic information. It is also a good example, however, of the way in which automation can limit or skew review. A search using the hyperlink will return only. On the other hand, "participant" searches from the DWS-EDMS search window using will return not only, but also.

If implemented before November 5, 2009, this revision would have had limited value to San Diego's review. Hasan's initial seven (7) messages to Aulaqi were not emails, but messages sent via the "Contact the Sheikh" function of Aulaqi's website. The website's internal email account then automatically transferred the messages by email to one of Aulaqi's email addresses. [The modification] would not have revealed those seven messages as part of the exchange between Hasan and Aulaqi. Moreover, reviewers might not have clicked on the link if [Hasan's communications] did not trigger a memory that he was the subject of a lead.

2. Automatic Flagging of [Certain Email Data]

STAS also modified DWS-EDMS on February 17, 2010, to automatically flag [certain email data]

[redacted] In the aftermath of the Fort Hood shootings, the FBI believed that [this email data could assist in identifying persons of potential interest] [redacted] [The flag] [redacted] is, of course, merely a visual cue and not, in and of itself, a basis for or indicator of any investigative action.

Conclusion: This modification provides a unique visual stimulus when [the FBI acquires email containing certain data] [redacted]. The flag also reminds the reviewer that contacts [redacted] may trigger the new [redacted] procedure outlined in Section [redacted].

If implemented prior to November 5, 2009, this change would not have assisted reviewers in identifying Hasan [redacted]

That said, this revision provides a useful visual cue for reviewers and should remain active.

3. Flagging DWS-EDMS Activity As [redacted]

On May 17, 2010, STAS implemented a [tool that allows DWS-EDMS users to flag certain communications regardless of the case in which these communications are located.] [redacted]

[redacted]

[The redacted portions describe details of sensitive FBI information systems.]

Conclusion: [redacted] This will provide a unique visual stimulus for

reviewers and also help coordinate Agents, Analysts, and TFOs working on the same or different cases.

If implemented prior to November 5, 2009, this revision would have allowed SD-Agent to create a means of flagging communications in DWS-EDMS. Like the other DWS-EDMS revisions, however, the tool is limited. As a result, the tool would not have flagged [certain of the Hasan-Aulaqi communications]; but it would have flagged [others].

This revision is vital. It provides an automated backstop to assure that [information is] not overlooked, as well as a means of notifying other Agents, Analysts, and TFOs [about information acquired] in their cases, creating additional synergy across investigations.

4. [Workload Reduction Tools]

STAS has developed [workload reduction tools] to assist reviewers in evaluating [DWS-EDMS information]. [These tools] identify [certain email data]

[The tools] do not replace human review but prioritize review based on potential importance. STAS is working with the FBI's Counterterrorism Division to refine and test [these tools].

The FBI has [used these tools] in DWS-EDMS on high profile cases, including the Aulaqi investigation.

Testing has revealed that. The DWS-EDMS [September 2011] release (see C.5 below) enables individual users to [adapt these tools] for their individual cases.

STAS also initiated a pilot project to develop a DWS-EDMS [tool] that would automatically identify [certain other email data]. The [tool] would not, but [would] assist reviewers in prioritizing products for review.

STAS tested the [tool] against the voluminous [information acquired] in the Aulaqi investigation. Recent tests indicate that the

[tool] is 96% to 98 % accurate . However, the [tool] has not been implemented. At this writing, the project is on hold given the need to focus limited STAS resources on more pressing matters.

Conclusion: The [tools] would assist users in organizing and prioritizing [information] for review without placing additional time or review demands on reviewers. Its primary drawback is .

5. **DWS-EDMS [September 2011] Release**

The [September 2011] release of DWS-EDMS is system evolution, not a remedy implemented as a result of the Fort Hood shootings. However, the [September 2011] release resolved many of our concerns about DWS-EDMS. We discuss it briefly here.

The [September 2011] release was deployed in beta format in May 2011 for feedback from a internal User Advocacy Group. Roughly 1,200 personnel given access to the application gave it an approval rating of 70%. Each user provided feedback, nearly all of which was incorporated into the application before its production release.

[The September 2011] release [is] the single common interface for all users. Training for the ten largest Field Offices was completed in December 2011. Feedback from the field has been overwhelmingly positive.

STAS deployed industry-leading third party tools for the development of [the] DWS-EDMS [September 2011 release] . The [September 2011] release includes a complete redesign of the user interface and resolves the performance and scalability issues that hamstrung earlier versions. It also provides Agents, Analysts, and Task Force Officers with automated analysis of cases and facilities as they work.

[redacted]

The [redacted] [September 2011] release deploys a new full text search capability- [redacted]

Conclusion: The [redacted] [September 2011] release is a vital improvement of DWS-EDMS that should ease and prioritize the workload of DWS-EDMS users. [redacted] We believe that [redacted] [the September 2011 release] represents a significant step forward for the system's software. As discussed in Part Five, we believe that a comparable step forward is [needed] for the system's hardware.

D. Training

In March 2010, the FBI instituted Headquarters and NJTTF oversight of JTTF training to ensure uniformity and quality of training across JTTFs and to ensure that Task Force Officers (TFOs) complete training promptly upon joining a JTTF. A mandatory four-day orientation course introduces new TFOs from partner departments and agencies to the FBI and JTTFs, including procedures for conducting and documenting investigations. New TFOs are taught that working in an FBI environment makes them responsible, like FBI personnel, for complying with the governing authorities, including those designed to protect civil liberties and privacy interests. The training also ensures that all TFOs understand and, if appropriate, have access to FBI databases that contain information relevant to their JTTF responsibilities.

On April 13, 2011, the Assistant Director of the Counterterrorism Division (CTD) reaffirmed and expanded the training requirements for all JTTF personnel, whether FBI Special Agents (SA), Intelligence Analysts (IA), and Staff Operations Specialists (SOS) or TFOs. The expanded training consists of three components· Virtual Academy training, classroom training and database training.

1. Virtual Academy

CTD identified twelve Virtual Academy training modules as the baseline level of training for JTTF personnel:

Joint Terrorism Task Force Orientation
FBI Watchlisting
FISA Accuracy
Information Sharing Environment (ISE) Core Training

Information Systems Security Awareness
Introduction to Domestic Terrorism
Introduction to International Terrorism
National Security Branch Introduction
National Security Letters (NSL)
Overview of Domestic Investigations and Operations Guide (DIOG)
Overview of the Attorney General Guidelines for Domestic FBI Operations
U.S. Persons and Information Sharing

These training modules are to be completed within 90 days after a SA, IA, SOS, or TFO is assigned to a JTTF. Personnel who do not complete this training within 90 days must complete all twelve modules immediately. Field Office executive management is required to ensure and document completion of the mandatory baseline Virtual Academy training modules.

2. Classroom Training

The NJTTF established the JTTF TFO Orientation & Operations Course (JTOOC) at Quantico to address TFO training needs. JTOOC is a five-day course designed to introduce TFOs to counterterrorism investigations. Classes are designed around a national counterterrorism case to assist discussion and interaction. All full-time TFOs, regardless of when assigned to a JTTF, who have not taken JTOOC are required to attend the course before October 2011. Part-time TFOs with unescorted access to FBI space and access to FBI computer systems are also required to attend the course. TFOs must complete all twelve baseline Virtual Academy training modules prior to attending JTOOC.

Field Office executive management is required to ensure that eligible TFOs assigned to their JTTF attend JTOOC and to document successful completion JTOOC by those TFOs.

3. Database Training

In 2010, in response to the FBI's initial Fort Hood investigation, CTD required that JTTF members to receive hands-on training on key FBI databases and systems, including the Data Warehouse System-Electronic Surveillance Data Management System (DWS-EDMS), Information Data Warehouse (IDW), Clearwater, and Automated Case Support (ACS)/Sentinel (see Part One, Chapter 4). In January 2010, a "train-the-trainer" session was conducted at Quantico. Each Field Office provided at least two trainers. These trainers then returned to their Field Office to train all TFOs, SAs, IAs and SOSs assigned to counterterrorism matters by March 2010. Training of JTTF members assigned after March 2010 is to be conducted within six months of access to FBI systems.

Conclusion: The FBI's post-Fort Hood enhancements of counterterrorism and JTTF training represent significant improvements. The critical shortfall before Fort Hood was the failure adequately to train Task Force Officers on their role as JTTF members and to provide them with knowledge about, and access to, FBI databases relevant to their responsibilities. We encourage the FBI to continue to focus on JTTF training in order to provide TFOs with all available tools and resources. It is also important to ensure that all TFOs understand that, regardless of their home agency, the FBI's governing authorities control their activities as JTTF members.

Part Four

Analysis of Governing Authorities

Existing Authorities

The Terms of Reference asked Judge Webster to "review ... whether current laws and policies strike an appropriate balance between protecting individual's privacy rights and civil liberties and detecting and deterring threats such as that posed by Major Hasan."

We discussed the FBI's governing authorities in Part One, 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 about the impact of the governing authorities on privacy rights and civil liberties.[10/] This Chapter assesses those concerns in the context of the FBI's responsibility to detect and deter terrorism.

We describe policy changes that the FBI has adopted. We also note areas that may need additional improvement or oversight. Congress is ultimately responsible for determining whether the appropriate balance exists. We believe our review will assist in that task.

The guiding principle of our analysis has been that, as the risk of potential infringement of individual privacy rights and civil liberties increases, the level of factual predication, supervisory approval, and oversight should increase. The FBI should monitor and report on its use of techniques that raise concern through OIC compliance reviews, Inspection Division audits, and National Security Division reviews. The FBI should modify or abandon policies and protocols that experience proves to be unacceptably harmful to privacy rights or civil liberties.[11/]

[10/] A letter to Judge Webster setting forth the ACLU's concerns is attached as Exhibit 1.

[11/] By letter dated December 9, 2010, Attorney General Eric Holder advised Senator Patrick J. Leahy, Chairman of the Senate Committee on the Judiciary, that DOJ and the FBI would implement certain enhanced privacy and civil liberties protections proposed in S. 1692, 111th Cong. (2009), the USA PATRIOT Act Sunset Extension Act, as reported by the Judiciary Committee. The Attorney General advised that he was "confident that these measures will enhance standards, oversight, and accountability, especially with respect to how information about U.S. persons is retained and disseminated, without sacrificing the operational effectiveness and flexibility needed to protect our citizens from terrorism and facilitate the collection of vital foreign intelligence and counterintelligence information." 157 Cong. Rec. S3,250 Ex. 1 (daily ed. May 24, 2011).

A. Standard for Opening Assessments/Investigative Techniques Used in Assessments

1. Background

The AG Guidelines authorized certain techniques in assessments that were not previously permitted during national security threat assessments, but were permitted for the "prompt and limited checking of leads" under the prior General Crimes Guidelines. The Attorney General promulgated this revision to better equip the FBI to detect and deter terrorist activity.

2. Concerns

To open an assessment, the FBI must identify its purpose in writing and that purpose must be "authorized," i.e., within the Bureau's mission. DIOG §§ 5.1-5.3. Critics are concerned that this standard authorizes the FBI to conduct assessments without any factual predicate suggesting the target's involvement in illegal activity or threats to national security. They believe the AG Guidelines and DIOG should require some factual predicate to avoid collecting and retaining information on individuals who are not engaged in wrongdoing.[12/]

A corresponding concern is that the AG Guidelines allow the FBI to use investigative techniques during an assessment that some regard as intrusive; for example, physical surveillance, recruiting and tasking informants to attend meetings under false pretenses, and engaging in "pretext" interviews in which Agents do not disclose their FBI affiliation and/or the purpose of the interview.

Commenters also believe the AG Guidelines "explicitly authorize the surveillance and infiltration of peaceful advocacy groups" prior to demonstrations and "open the door to racial profiling." Letter from Laura W. Murphy, Director, ACLU Washington Legislative Office, and Anthony D. Romero, Executive Director, ACLU, to Hon. William H. Webster (August 6, 2010) at 7. They believe the AG Guidelines should be amended to provide stronger protection of First Amendment activity and to ban racial profiling.

12/ Based on data obtained from the FBI under the Freedom of Information Act, a recent news article reports that the FBI opened 82,325 Type 1 & 2 assessments of persons or groups between March 25, 2009, and March 31, 2011. Charlie Savage, F.B.I. Focusing on Security Over Ordinary Crime, *New York Times*, August 24, 2011, at A16. Information collected in those assessments led to 3,315 preliminary or full investigations that remained open as of May 2011. The FBI also opened 1,819 Type 3 assessments during that period to identify particular threats in particular geographic areas. 1,056 remained open in May 2011. Based on this data, the ACLU has expressed concern that the FBI is "casting its investigative net too broadly" and that the assessment authority granted by the AG Guidelines is "far too broad." Id. Valerie Caproni, then-FBI General Counsel, noted that the data showed that the FBI had disposed of about 96 % of the assessments using "low intrusion techniques" without opening a potentially more invasive preliminary investigation. Id.

3. Evaluation

We believe that the increased flexibility under the AG Guidelines to conduct assessments using specified techniques is critical to the FBI's ability to combat terrorism. The FBI's evolving role as an intelligence agency demands anticipation rather than reaction. If the Bureau's ability to gather information were limited to circumstances of specific factual predication, then in many cases it would not be able to identify and prevent threats before they escalate into action. Without the ability to gather and analyze intelligence, the FBI would be primarily reactive, investigating crimes and terrorist acts after they occur.

We recognize, however, that the AG Guidelines standard for opening counterterrorism assessments and conducting investigative activity can lead to the collection of information about individuals who turn out not to have been involved in any illegal or terrorist activity. We discussed this issue with the FBI and reviewed its safeguards for minimizing the collection and retention of such information.

First, the DIOG prohibits assessments based on "arbitrary or groundless speculation"; solely on the exercise of First Amendment rights; solely on the race, ethnicity, national origin, or religious practice of any person or group; or on a combination of only these factors. These front-end prohibitions are closely enforced and monitored by the FBI.

Second, the Privacy Act prohibits the retention of information about how First Amendment rights are exercised unless it relates to criminal activity or a national security threat. See 5 U.S.C. § 552a(e)(7). FBI policy sets out procedures for removing information from FBI records that does not comply with the Privacy Act. See Corporate Policy Notice 0356N, Handling of Information Gathered in Violation of the Privacy Act (effective June 9, 2011).

Third, as noted in Chapter 4, the FBI's Guardian Threat Tracking system is an access-controlled classified database that provides terrorism threat tracking and management for all Type 1 & 2 assessments and all incidents with a potential nexus to terrorism (including those that lead to predicated investigations). FBI policy requires the entry of all terrorism-related threats, events, and suspicious activities into Guardian. The Guardian Management Unit (GMU) is responsible for administering the system and for ensuring that all policies involving the types of information that can be entered into Guardian are followed. GMU's Assessment Review Team (ART) reviews each Guardian assessment to ensure that there was a sufficient basis to open the assessment (i.e., an authorized purpose not based solely on protected rights or characteristics); that only authorized techniques are used; and that all applicable DIOG and FBI policies are followed, including those policies that proscribe the retention of information that is inconsistent with the Privacy Act. When ART identifies a compliance issue, it follows up with the Field Office involved and is authorized to seek the removal of improperly collected or retained information from FBI systems.

Fourth, the FBI has initiated the process to shorten the 30-year retention period for information collected through Guardian leads. Under the new policy, this information will be accessible for five years. If there are no "hits" against the information, it will be available only on a restricted basis for an additional five years. Users will receive notification of any hit, but will need to obtain a supervisor's permission to access the information. If there are no hits after

ten years, the information will be removed from the system. Under the Federal Records Act, the FBI is required to obtain approval of the change through the National Archives and Records Administration.

Fifth, FBI policy requires that reviewing Agents who determine conclusively that no nexus to terrorism exists must note "No nexus to terrorism" when closing a Guardian lead. This serves two purposes. If the FBI receives similar complaints involving the individual or group, reinvestigation may not be necessary. If the subject becomes involved in illegal or terrorist activity, there will be a record of the previous encounter.

There is also oversight. Type 3 through 6 assessments require the approval of a Supervisory Special Agent or Supervisory Analyst, who must be satisfied that (1) the basis of the assessment is well-founded (which typically means supported by source information, intelligence reporting, information from other agencies or foreign partners, or public source data); and (2) there is a rational relationship between the stated purpose of the assessment, the information sought, and the means proposed to obtain that information. Type 1 & 2 assessments, which involve the prompt and limited checking of leads, do not require supervisory approval unless they involve a "sensitive investigative matter" (SIM). A supervisor must assign Type 1 & 2 assessments. which requires the supervisor to review the assessment. He or she must close the assessment if there is no valid basis for action.

In addition, all assessments are subject to regular file reviews at least four (4) times per year in which the supervisor must determine whether the assessment should remain open.[13] Legal counsel and the Special Agent in Charge (SAC) must review and approve any assessment involving a SIM, which includes investigations of domestic public officials or political candidates involving corruption or threats to national security; religious or domestic political organizations (including organizations formed to advocate or educate the public about a political or social issue) and persons prominent in them; the news media; an investigative matter having an academic nexus; and any other matter that in the judgment of the official authorizing the investigation should be brought to the attention of FBI Headquarters. DIOG 2.0 §§ 10.2.1, 10.1.3. Further, the technique(s) used in all assessments and predicated investigations must be the least intrusive feasible means, that are operationally sound and effective, of securing the desired information sufficient to meet the investigative objective (for example, physical surveillance should not generally be used when accurate information can be obtained from public sources). DIOG § 4.4; see also AG Guidelines I(C)(2)(a); Exec. Order No. 12333 at § 2.4 (Dec. 4, 1981). DIOG 2.0 § 10.1.3 requires that "particular care" should be taken in a SIM when considering whether the planned course of action is the least intrusive means.

Certain assessment techniques deserve discussion. Although expressed concerns about these techniques have focused on their use in assessments, some extend to their use in predicated investigations.

13/ When the DIOG became effective, OIC instituted a compliance monitoring program that required operational program managers to review 10 assessments per program per week to ensure compliance with the DIOG. That program was discontinued in light of the positive results of the Inspection Division's 2009 audit of the FBI's use of assessments and the Inspection Division's plans to conduct future audits of DIOG compliance.

Physical Surveillance. Physical surveillance can occur only in areas where there is no constitutionally protected expectation of privacy and requires an articulated purpose and a supervisor's authorization. There is a [redacted] [time] limit on physical surveillance. DIOG § 5.9.B.2. [Each request of physical surveillance must be justified and approved by a supervisor.] [redacted] [The redacted portions contain information that would disclose techniques and procedures for law enforcement investigations and prosecutions.] The goal of these controls is to permit Agents to respond to leads quickly and effectively or to obtain the limited factual information necessary to achieve the purpose of the assessment while precluding long-term, continuous surveillance of a person's lifestyle or habits when there is no basis for opening a predicated investigation.

Source Recruitment. To facilitate the prompt and limited checking of leads, the prior General Crimes Guidelines authorized recruiting and tasking sources without an open investigation; but the AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection prohibited these techniques during national security threat assessments. The DIOG, based on the authority provided by the Attorney General Guidelines, authorizes these techniques for assessments across all FBI investigative programs. Source recruitment, vetting, and validation are critical to the FBI's success as an intelligence agency. Although the AG Guidelines expanded the range of techniques available for source recruitment (to include use of false identification, voluntary polygraph examinations, and searches that do not require a court order), the FBI did not authorize use of these other techniques until it finalized policies governing their use.

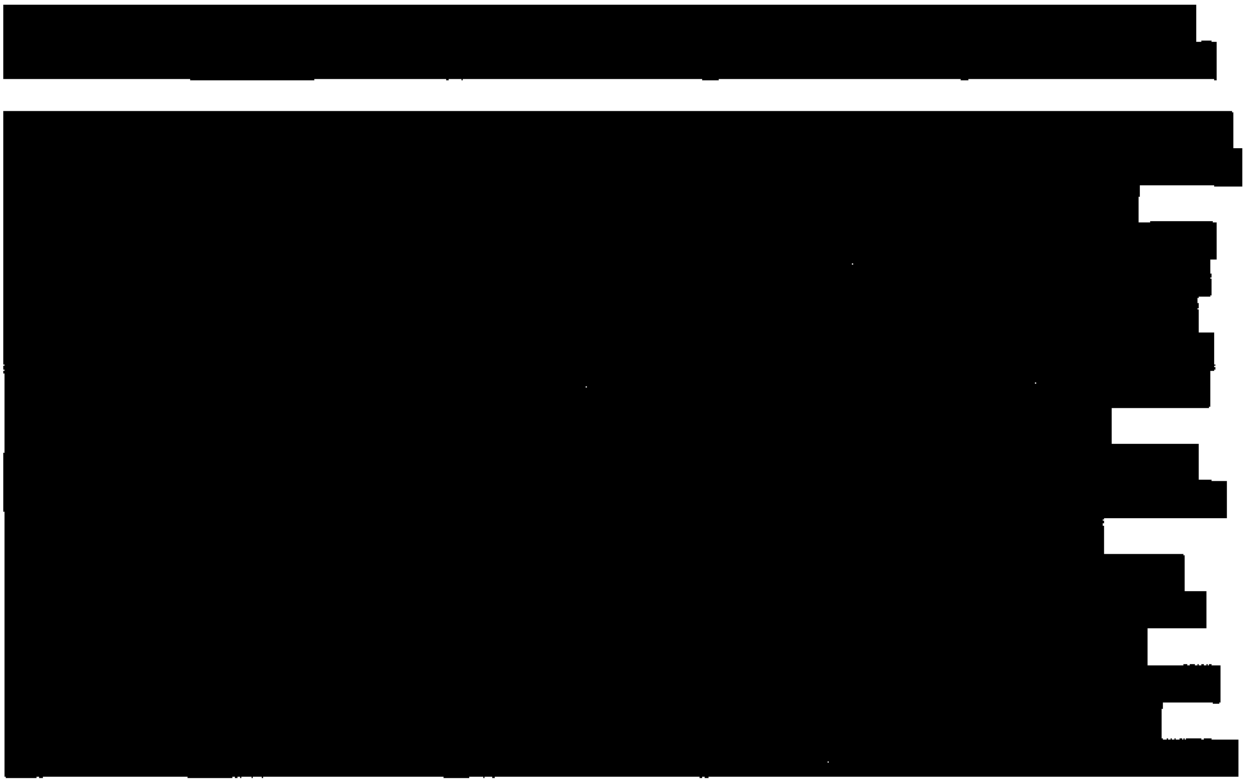
Interviews. In its discussion of least intrusive means, the DIOG recognizes that an FBI interview of an individual's employer, family, or other acquaintances could, in certain circumstances, create a risk of harm to the individual arising from the contact itself or the information sought. DIOG § 4.4.C.5. In recognition of this risk, the FBI has cautioned its personnel that, when determining the least intrusive means, they should consider the intrusiveness of conducting an interview of a subject's employer (among others). Id. Consistent with this guidance, the Supervisory Special Agent and Task Force Officer (TFO) who conducted the Washington, D.C., JTTF assessment of Nidal Hasan cited the potential adverse impact on his military career as a reason they did not contact his superiors at Walter Reed Army Medical Center. We recognize that Agents and TFOs face a difficult task in balancing the competing interests in this situation. If no interviews are conducted, they risk being criticized for failing to act to prevent harm. If they conduct an interview and harm to the individual results, they risk criticism for causing that harm. We believe that the DIOG's existing guidance is appropriate, and we encourage the FBI to remain sensitive to minimizing potential harm when conducting interviews.

"Pretext" Interviews. FBI policy limits the circumstances in which Agents may conduct an interview without affirmatively disclosing their FBI affiliation or the purpose of the interview. DIOG § 5.9.F.4. During an assessment [redacted]

[redacted] [FBI employees] are not permitted to conduct a formal interview using a false identity or [false purpose. They also may not] engage in "Undercover Activity" during an assessment. (The Attorney General's Guidelines for Undercover Operations define an "Undercover Activity" as "any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI.") Agents must also consider whether a pretext interview is the least intrusive means of gathering the information needed.

Undisclosed Participation. Pursuant to Executive Order 12333, no one acting on behalf of the U.S. Intelligence Community may join or otherwise participate in an organization in the U.S. without disclosing his or her affiliation except in accordance with procedures approved by the Attorney General. On November 26, 2008, the Attorney General, in consultation with the Director of National Intelligence, signed the policy that governs the undisclosed participation (UDP) of FBI employees and sources in U.S. organizations and business entities. The DIOG incorporates this policy. DIOG § 16.1.A. [redacted] UDP that is likely to affect First Amendment rights may occur only during a predicated investigation and must comply with the least intrusive means principle and any other investigative requirements that apply.

In light of the sensitivity of UDP activity involving religious [, advocacy, and similar] organizations, we examined FBI policy governing that activity. We learned that the level of required approval is generally proportional to the intrusiveness or sensitivity of the activity. [redacted] DIOG 2.0 §§ 16.1.3, 16.3. [redacted]



[The redacted portion sets forth the escalating approvals required by FBI policy for UDP; the more sensitive the activity, the higher the approval level. These approvals may include a Supervisory Special Agent, Chief Division Counsel, or other DOJ or FBI lawyers, a Special Agent in Charge, an FBI Assistant Director, or the Director.]

Given this infrastructure and heightened approval levels, we believe that the FBI has appropriately balanced the protection of national security with privacy rights and civil liberties in its use of UDP. We recommend, however, that OIC and the Inspection Division monitor the FBI's use of UDP in these contexts to ensure that the balance holds.

Racial Profiling. Racial profiling, or the invidious use of race or ethnicity as the basis for targeting suspects or conducting stops, searches, seizures, and other investigative procedures, has no place in law enforcement. It is an unconstitutional and ineffective law enforcement tool. It is also prohibited by FBI policies. The DIOG incorporates the DOJ Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, which prohibits racial profiling and describes the limited circumstances in which law enforcement may consider race or ethnicity. Chapter 4 of the DIOG provides extensive guidance designed to prevent racial or ethnic profiling. It prohibits the use of race or ethnicity as the primary, dominant, or sole factor in commencing an assessment or investigation.

Race and ethnicity may be used as a specific identifier of a suspect based on credible information. If the FBI receives a lead that a short, white male robbed a bank, the FBI can limit the pool of suspects to short, white males without running afoul of prohibitions on racial or ethnic profiling. Race or ethnicity also may be considered if it has an explicable and well-founded nexus with the threat or group being assessed or investigated; for example, some

criminal gangs and terrorist organizations consist exclusively or primarily of persons of a common ethnic background.

The prohibition of investigative activity based solely on race or ethnicity also applies to the collection of racial/ethnic demographics and behavioral characteristics. The DIOG allows collection of this information only for limited purposes, such as furthering intelligence analysis and planning around potential threats and vulnerabilities.[14/]

Undercover Operations and Activities.

[redacted]

[The redacted portion describes the various FBI committees that must approve undercover counterterrorism operations and activities involving sensitive circumstances; one committee includes mid-level FBI managers, and the other includes senior executives (discussed below). Both include lawyers from the DOJ.]

At the Director's request, the FBI also established the Sensitive Operations Review Committee (SORC) chaired by the [redacted]. Its members include Assistant Directors or designated Deputy Assistant Directors for various investigative divisions, [redacted] and the Assistant Attorneys General of the [redacted] or their senior level designee. Advisors include the FBI Corporate Policy Office and DOJ Chief Privacy and Civil Liberties

---

14/ For example, collecting demographics about a concentrated ethnic community could enable a Field Office to assess and mitigate the threat posed by an ethnically-identifiable terrorist organization's efforts to recruit new members from that community. The data could also be mapped to enable the identification of otherwise imperceptible connections. Moreover, knowing that terrorist groups recruit members from a certain region of the ethnic group's home country (ethnic behavioral information) would be relevant to the assessment [redacted]. In these examples, the rationale for collection is not based solely on the community's ethnicity. Because of the potential risk of harm to civil rights and liberties in the collection of such information, we recommend that OIC and the Inspection Division monitor these collections to ensure that harm does not occur.

Officer or a designee. The SORC reviews and makes recommendations to the Director on sensitive operations and initiatives (whether assessments or investigations), including sensitive UDP; for example, the SORC reviewed a proposed undercover operation during an investigation that would attract predicated subjects but also might require substantial interaction with members of the general public. The DIOG requires notice to the SORC of less sensitive operations and initiatives to ensure high-level monitoring, trend evaluation, and reports to higher authority. This level of review is important for sensitive activities during assessments, which are limited; for example, undercover activity is not allowed in an assessment.

In certain recent counterterrorism cases, the FBI used a CHS or an undercover FBI employee (UCE) in dealing with individuals who were later arrested. Given concerns about whether CHS or UCE use in these circumstances comports with the law and judicial precedent on entrapment, we examined FBI policy. The FBI uses CHSs and UCEs to gather intelligence in ongoing predicated investigations; more rarely, a CHS (but not UCE) may report on the subject of an assessment. FBI personnel who approve CHS and UCE use are obligated to assure there are safeguards to protect the rights of those affected. When the FBI receives an allegation or lead indicating that an individual may be planning or is interested in committing a terrorist act, the FBI structures and monitors the investigation to confirm the subject's required predisposition to engage in criminal activity and to avoid unlawful entrapment. This is accomplished in part by involving FBI and National Security Division attorneys (as well as a local AUSA) when the disruption plan may involve a criminal prosecution. The attorneys evaluate the prospect of prosecution and[, if so,] how best to conduct the investigation to enhance the likelihood of success while ensuring that individuals are not lured into criminal activity. This may include, for example, providing the subject with clear opportunity to opt out of criminal conduct.[15/]

Given the substantial involvement of FBI and DOJ attorneys and the required higher levels of approval, we believe the FBI's use of undercover operations and activities in counterterrorism investigations is properly administered. We also believe that the rights of individuals not involved in or predisposed to terrorist or criminal activity are safeguarded. We recommend, however, that OIC and the Inspection Division monitor undercover operations and activities, including CHS and UCE use, in counterterrorism investigations to ensure that those rights continue to be protected.

DIOG 2.0. Concerns also have been expressed that certain DIOG 2.0 revisions provide the FBI with leeway to infringe privacy rights. For example, there is concern that permitting Agents to search commercial or law enforcement databases (i.e., a "record check") before an assessment is opened without making a record of the inquiry could result in inappropriate use of databases. The purpose of this change, however, was to enable Agents to run quick checks on individuals (for example, in response to a citizen complaint) and resolve unfounded complaints while preserving resources and minimizing the impact on the subjects of complaints. DIOG 2.0

15/ To assure their reliability, all new CHSs are subject to an extensive investigation of their background, access to information, and character [as well as periodic validation]. [redacted]

§ 5.1.2 requires that "FBI employees must document and retain records checks . . . if, in the judgment of the FBI employee, there is a law enforcement, intelligence or public safety purpose to do so." Otherwise, the results of record checks cannot be retained. [redacted] [Also, widespread media reports have invited public scrutiny of the FBI's possible use of voluntary lie detector tests and trash covers when evaluating a potential informant, the multiple use of surveillance squads in an assessment, and the number of times Agents or informants can attend group meetings before the UDP rules apply. Any such changes would be] [redacted] within the scope of authority granted by the AG Guidelines. The FBI imposed restrictions on using [redacted] [certain] techniques until policy guidance could be developed. However, given the potential risks to civil liberties and privacy, we recommend that OIC and the Inspection Division monitor the use of the additional investigative techniques authorized by DIOG 2.0 to ensure that a proper balance has been struck.

* * *

Based on this combination of controls, we believe that assessments using the authorized techniques should not result in the intrusive collection or retention of personally identifiable information about large numbers of U.S. persons for impermissible reasons or infringe privacy rights or civil liberties.

Our conclusion is supported by an Inspection Division audit of all Type 3 through Type 6 assessments pending in 2009 in seven compliance areas: monitoring of First Amendment activities; collection of information based on protected characteristics; assessments based solely on FBI national or field office collection requirements; identification of assessments as SIMs; approval for undisclosed participation; approval of authorized investigative methods; and use of prohibited investigative methods.

Of the 3,426 assessments evaluated, only 178 (5.2%) had one or more of a total of 218 compliance errors. No assessment collected information based on protected characteristics. The 218 compliance errors involved identification of assessments as SIMs (158); FBI Headquarters and Field Office collection requirements (35); approval of authorized investigative methods (17); monitoring of First Amendment activities (3); approval for UDP (3); and use of prohibited investigative methods (2). Of the 218 errors, 213 (98%) were administrative and primarily involved Field Office failure to recognize and designate an assessment as a SIM (158 errors) or assessments based solely on collection requirements (35 errors). The other five errors were substantive and mainly involved initiating an assessment or retaining information during an assessment that appeared to be based solely on First Amendment activities. The audit determined whether those assessments were based on an authorized purpose and collected information related to that purpose. The FBI closed assessments that were not in compliance and/or removed and sequestered the information collected.

In September 2010, OIG reported on the FBI's investigation of domestic advocacy groups. OIG found no evidence that the FBI had targeted any group or individual based on First

Amendment activities. The report concluded that the FBI had generally predicated the investigations on concerns about potential criminal acts rather than First Amendment views. OIG found that the FBI's purpose for attending a 2002 anti-war rally fulfilled the AG Guidelines, but that FBI statements to Congress and the public tying attendance to an FBI subject were inaccurate and misleading. OIG criticized the factual basis for opening or continuing domestic terrorism investigations of certain non-violent advocacy groups and questioned classifying some cases as domestic terrorism and opening some investigations as full rather than preliminary. OIG also found instances of questionable investigative techniques and improper collection and retention of First Amendment information.

The report noted that the AG Guidelines had loosened prior limitations on FBI retention of information collected in connection with public events, which had been prohibited unless related to potential terrorism or criminal activity. OIG recommended that the FBI consider reinstating the prohibition. In a September 14, 2010, letter from Deputy Director Timothy P. Murphy to the Inspector General, the FBI concurred with this recommendation and the report's other recommendations.[16/]

4. Recommendations

Although we conclude that the AG Guidelines standard for opening an assessment and the available investigative techniques strike an appropriate balance, privacy rights and civil liberties may be implicated. We recommend that OIC and the Inspection Division conduct compliance reviews and audits on a regular basis – at least annually, for a period of three years – of the FBI's use of assessments and the investigative techniques used to ensure compliance with policies and procedures that guard against the inappropriate use of race, ethnicity, national origin, or religion as a basis for investigative activity and to identify any concern about or impact on privacy rights and civil liberties.

Because assessments may collect information that has no current investigative value, we further recommend that the FBI strictly adhere to policies to ensure that personnel do not access or view this information without a legitimate law enforcement or intelligence reason. These policies include the requirement that any investigative activity – including activity involving assemblies or associations of U.S. persons exercising their First Amendment rights – must have an authorized purpose under the AG Guidelines that is rationally related to the information sought and the technique to be employed. DIOG § 4.2.D. We recommend that the FBI apply these policies with particular focus – and OIC monitoring – on information gathered during

---

16/ Information concerning the exercise of First Amendment rights by U.S. persons may be retained only if pertinent or relevant to FBI law enforcement or national security activity. DIOG 1.0 § 5.13; DIOG 2.0 § 5.12. DIOG 2.0 §4.1.3provides that documents describing First Amendment activity that are determined to have been collected or retained in violation of the Privacy Act must be destroyed, citing Records Management Division Policy Notice 0108N. The Privacy Act forbids federal agencies from collecting information about how individuals exercise their First Amendment rights, unless authorized by statute or by the individual, or it is pertinent to and within the scope of authorized law enforcement activity.

assessments that implicates privacy interests or civil liberties or that relates to First Amendment activities or other Constitutional rights.[17]

B. National Security Letters

1. Background

After the PATRIOT Act revised the standard for issuing National Security Letters (NSLs) to "relevance to an authorized investigation" and the FBI significantly increased the number of Special Agents assigned to counterterrorism, the FBI's use of NSLs increased from 8,500 in 2000 to an average of about 19,000 per year from 2008 to 2010. The FBI has used information obtained through NSLs to determine whether further investigation is needed; to generate leads for Field Offices, JTTFs, and other federal agencies; to prepare FISA applications; to corroborate information developed through other investigative techniques; and to clear individuals suspected of posing a threat to the national security.

In 2006, Congress amended the NSL statutes to provide the government with explicit enforcement authority and to respond to, among other things, the Southern District of New York's decision in Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), and other judicial decisions that had questioned the constitutionality of the non-disclosure provisions. The amendments also required two DOJ Inspector General (OIG) audits of the FBI's use of NSL authority.

2. Concerns

The OIG audits shaped much of the public perception of NSLs. The OIG's March 2007 report found that, prior to 2007, the FBI had inadequate internal controls on NSLs and had not adequately trained personnel to understand the intricacies of the statutes. These inadequacies led to a small, but not insignificant, number of NSLs being issued inappropriately. The OIG's March 2008 report noted that the FBI had made significant progress in rectifying the problems identified in 2007. The OIG found no intentional violations of the governing authorities, although one Headquarters unit had circumvented protections in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), by issuing over 700 "exigent

---

[17] Although our recommendation concerns information gathered during assessments, the FBI should consider monitoring its compliance policies for all information collected that lacks current investigative value and implicates privacy rights and civil liberties. We considered whether front-end access control procedures similar to the NSL Procedures discussed below should apply to such information. We determined that those protocols would not be practical because the limited search capabilities of the FBI's current technology could effectively render information stored in a discrete database inaccessible. Data aggregation and integration of lawfully obtained information are critical to the FBI's counterterrorism mission. The need for strict compliance and OIC monitoring is underscored by recent news reports that the ACLU has obtained documents from the FBI through the Freedom of Information Act that reflect the improper retention of First Amendment activity information in violation of the Privacy Act. *Washington Post*, Dec. 2, 2011, at A3.

letters" for telephone billing information. That unit's actions were the subject of a 2010 OIG report. The FBI had prohibited the use of exigent letters before OIG issued its 2007 report.

Critics believe the PATRIOT Act unwisely loosened the nexus between the information sought by an NSL and the factual basis for suspecting activity that threatens national security. They say the statutory standard ("relevance to an authorized investigation") permits the FBI to obtain records about subjects with no ties to an agent of a foreign power (for example, a terrorist organization). These critics believe the FBI should have reason to believe that the subject of the records has some connection to an agent of a foreign power or to his or her activities. Critics also argue that certain transactional records such as to-and-from calling information should be available only with a Section 215 court order or a grand jury subpoena because these records are more sensitive than basic subscriber information (name, address, and billing information). Critics suggest that the statutory non-disclosure provisions are overbroad and should be amended to reflect Doe v. Mukasey, 549 F.3d 861 (2d Cir. 2008); require the government to demonstrate that national security would be harmed in the absence of the non-disclosure order; and automatically nullify the order when the threat ceases to exist.

The Senate Judiciary Committee proposed legislation in 2010 (S. 1692) to address certain concerns about NSL authority by (1) allowing the recipient of a non-disclosure order to challenge that order at any time; (2) requiring the FBI to retain a statement of facts showing that the information sought is relevant to an authorized investigation; and (3) requiring the Attorney General to establish procedures for the handling of NSL-obtained information. The proposed legislation would have included a four-year sunset provision.

3. Evaluation

These concerns are important. We are satisfied, however, that the FBI has implemented procedures and policies to resolve the compliance issues identified by the OIG. The most significant solutions are the addition of an automated NSL workflow subsystem to the computerized FISA management system and the implementation of the NSL Procedures.

NSL Subsystem. The NSL subsystem became operational in all Field Offices and Headquarters on January 1, 2008. It is used to generate and seek approval of most NSLs, and ensures that the FBI can issue NSLs only after invoking the appropriate statutory authority, obtaining all required approvals (including legal review), and opening an investigative file in accordance with the AG Guidelines. No NSL prepared in the subsystem can be approved or issued without all requisite information, such as the subject of the NSL, the predication, the type of NSL requested, the recipient, and the target(s). (With OGC approval, limited categories of NSLs can be created outside of the subsystem. Separate procedures, including a regular review of those NSLs, promote compliance with statutory and policy requirements.)

The FBI supplemented the NSL subsystem with published guidance that stresses the least intrusive means doctrine and defines the scope of review by FBI attorneys and signatories. FBI attorneys must review a proposed NSL to determine whether the data sought is relevant to a national security investigation, and the investigation appears to be properly predicated. The signer of the NSL, generally the SAC or Acting SAC of a Field Office, must determine whether the information is relevant to the investigation, the investigation appears to be adequately

predicated and, if applicable, there is a valid basis to impose a non-disclosure requirement. Because the NSL subsystem is role-based, only persons with identified authority can approve NSLs. The Inspection Division periodically samples NSLs to confirm, among other things, that NSLs are properly authorized.[18/]

NSL Procedures. In response to the OIG's 2007 report, Attorney General Gonzales convened a NSL Working Group to examine (1) minimizing the retention and dissemination of NSL-derived information; (2) "tagging" (segregating or marking) NSL-derived information in databases for tracking and, if necessary, deletion; and (3) limiting the retention of NSL-derived information. On October 1, 2010, Attorney General Holder approved the Working Group's proposed National Security Letter Procedures. The FBI incorporated the Procedures into DIOG 2.0. DIOG 2.0 § 18.6.6.3.12.

The NSL Procedures govern the collection, use, and storage of NSL-derived information and are designed to ensure that only those records that may have "investigative value" are included in the Automated Case Support (ACS) system, which houses FBI investigative case files and is generally available to almost all FBI employees with investigative or analytic responsibilities. (Having "investigative value" means the information responds to or creates a new investigative need, contributes to an intelligence collection requirement, or has the reasonable potential to provide other FBI or Intelligence Community employees information of value, consistent with their mission.)

The NSL Procedures require FBI employees to determine that material uploaded to ACS is responsive to the NSL and will serve the goals of the investigation or reasonably can be expected to serve the goal of other investigations. Only NSL-derived information that is responsive to the NSL and which has potential investigative value may be uploaded to ACS. However, all NSL-derived information may be entered temporarily as electronic files on the hard drives of desktop computers to determine whether it is responsive and has investigative value. Because desktop computers are accessible only with a password, other employees cannot access information stored on the hard drives. All records that lack current investigative value, but which fall within the scope of the NSL request, are preserved in the physical file (with controlled access) to ensure that, in the event subsequent information or analysis renders the records relevant to an FBI investigation or Intelligence Community need, they will be accessible.

[18/] The Inspection Division evaluated the effectiveness of the NSL subsystem by auditing random samples of 699 NSLs issued in 2008; 1,560 NSLs issued in 2009; and 1,499 NSLs issued in the first half of 2010. The audits also included all NSLs created outside of the NSL subsystem. The Inspection Division determined that six (0.9%) of the 2008 NSLs, ten (0.7%) of the 2009 NSLs, and eleven (0.7%) of the 2010 NSLs had errors requiring a Possible Intelligence Oversight Board (PIOB) violation referral to the OGC and the National Security Law Branch. The errors were classified into three principal types: improper authorization (5), overproduction and unauthorized use (10), and substantive typographical error (4). A few administrative errors resulted from FBI policy lapses that did not rise to a PIOB violation. The overall administrative error rate was 4.7% for 2008; 0.9% for 2009; and 0.1% for the first half of 2010. The FBI attributes the significant reduction in errors to the NSL subsystem.

The NSL Procedures contemplate the potential creation of a discrete, secure database for storing and analyzing financial information to identify connections of interest that might not otherwise be apparent. Any such database would have access controls, an established access policy, and an audit capacity to monitor compliance.

Documentation and Non-Disclosure Provisions. The DIOG also requires the FBI to prepare and retain a statement of facts showing (1) that the NSL seeks information relevant to an authorized investigation; and (2) if applicable, the need for a non-disclosure order. DIOG § 11.9.3.E. As of February 2009, all NSLs that invoke the non-disclosure provisions must include a notice informing recipients of the opportunity to challenge the non-disclosure requirement through government-initiated judicial review. The NSL subsystem automatically generates this notice. Id. If a recipient unsuccessfully challenges a non-disclosure order, the FBI will review the continued need for non-disclosure and notify the recipient when compliance with the order is no longer required. Thus far, there have been only four challenges to non-disclosure. In two challenges, the FBI permitted the recipient to disclose its receipt of an NSL.

In our view, the FBI's implementation of OIG's recommendations, adoption of the NSL subsystem, policy guidance, and the NSL Procedures provide an appropriate balance between the FBI's national security needs and privacy rights and civil liberties. We recognize that the PATRIOT Act's "relevance to an authorized investigation" standard can produce NSLs that acquire information that later proves irrelevant to national security investigations. However, this standard enhances the FBI's ability to acquire and assess intelligence in an effective and timely manner and matches the standard that applies in criminal investigations. Moreover, NSLs can be issued only in predicated investigations, not in assessments, thus assuring their use only in investigations involving suspected criminal or terrorist activity.[19/]

4. Recommendation

To ensure that the FBI's procedures minimize the risk to privacy rights and civil liberties, OIC and the Inspection Division should regularly conduct, as experience indicates, compliance reviews and audits of the FBI's use of its NSL authority and the efficacy of the document control and access procedures.

[19/] OIG is reviewing NSL use from 2007 to 2009 and the FBI's progress in responding to earlier OIG recommendations. OIG also intends to examine the NSL subsystem. The DOJ National Security Division and OGC monitor the FBI's use of NSLs and the document handling procedures as part of periodic National Security Reviews. In addition, DOJ and the Office of the Director of National Intelligence will soon complete the joint report to Congress on NSL minimization required by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

C. FISA Section 215 Business Records Authority

1. Background

FISA Section 215 business records authority is a national security tool parallel to criminal discovery tools (for example, grand jury subpoenas). The operational requirements of most national security investigations require the secrecy afforded by FISA rather than the more limited confidentiality available in criminal investigations.[20/]

2. Concerns

Critics say that Section 215, like the NSL statutes, uses a standard ("relevance to an authorized investigation") that inappropriately loosens the nexus between the order sought and the factual basis to suspect activity that threatens the national security. They also suggest that the statutory presumption of relevance to an authorized investigation – which applies if the government shows that the records sought pertain to (a) a foreign power or the agent of a foreign power; (b) the activities of a suspected agent of a foreign power who is the subject of an authorized investigation; or (c) an individual in contact with, or known to, an agent of a foreign power who is the subject of an authorized investigation – is unnecessary and enables the government to secure FISC approval without providing facts to support the request.

The Senate Judiciary Committee proposed legislation in 2010 (S. 1692) that would have addressed these concerns by (1) removing the statutory presumption of relevance; (2) requiring the government to provide a statement of facts to the FISC supporting its belief that the records sought are relevant to an authorized national security investigation; (3) heightening the standard for library circulation/patron lists ("reasonable grounds to believe the tangible things [sought] are relevant to an authorized national security investigation and pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent of a foreign power, or (c) an individual in contact with or known to such an agent"); and (4) authorizing the FISC to review compliance with the minimization procedures.

Critics also argue that Section 215 runs afoul of the Fourth Amendment by allowing the government to obtain records by showing "relevance to an authorized investigation" rather than "probable cause." However, a Section 215 order is not a "search" within the meaning of the Fourth Amendment. E.g., Zurcher v. Stanford Daily, 436 U.S. 547, 563 (1978) (grand jury subpoenas "do not require proof of probable cause"); Okla. Press Pub. Co. v. Walling, 327 U.S. 186, 195 (1946) (orders for the production of records "present no question of actual search and seizure").

20/ From 2001 to 2010, the FISC issued more than 380 Section 215 orders. Nearly half of these orders were issued in 2004-2006 in tandem with FISA pen register orders because a statutory anomaly prevented automatic acquisition of subscriber identification information associated with telephone numbers identified by the pen register/trap-and-trace. Congress corrected this deficiency in the USA PATRIOT Act Additional Reauthorizing Amendments of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006). The other Section 215 orders obtained hotel, rental car, shipping, and similar records.

3. Evaluation

Congress built safeguards against misuse into Section 215. Section 215 orders are more protective of civil liberties than the grand jury subpoenas routinely issued by federal prosecutors. Section 215 orders, like grand jury subpoenas, can only seek records relevant to an authorized investigation; but a Section 215 order requires court approval, while a prosecutor can issue a subpoena without judicial review. Moreover, a Section 215 order may not issue if the investigation of a U.S. person is conducted solely on the basis of First Amendment activities. Finally, Section 215 requires the DOJ to submit detailed reports to Congress about its use.[21/]

Congress added further safeguards to Section 215 in the Reauthorization Act of 2006, requiring high-level FBI approval (Executive Assistant Director for National Security) before a Section 215 order could be sought for "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person." 50 U.S.C. § 1861(a)(3). Congress also added procedures allowing the recipient of a Section 215 order to challenge its validity and the basis for its non-disclosure requirement by appeal to the FISC. To date, no recipient of a Section 215 order has challenged its validity.

Consistent with prior FBI policy and FISC practice, the DIOG does not rely on the presumption of relevance; it requires the preparation and retention of a written statement of facts supporting all Section 215 business records applications to the FISC. DIOG 2.0 § 18.6.7.3.3. DOJ, in consultation with the FISC, is developing minimization procedures to replace the interim procedures governing the handling of materials obtained under Section 215.

We believe that FISA's protective provisions and the FBI's policy guidance appropriately balance national security investigative needs with privacy rights and civil liberties. We recognize that the "relevance to an authorized investigation" standard can result in the acquisition of information that proves irrelevant to national security investigations. That standard is necessary, however, to ensure that the FBI can acquire and assess intelligence in an effective and timely manner. As Attorney General Holder has noted, 50 U.S.C. § 1861(b)(2)(B) requires minimization procedures for Section 215 orders. The FBI is operating under interim procedures pending the FISC's adoption of formal procedures. We endorse the DOJ's effort to finalize proposed formal procedures. We anticipate that those procedures will minimize the risk that access to irrelevant information may pose to civil liberties and privacy interests. Finally, the NSD will continue to monitor the FBI's use of Section 215 authority and its application of minimization procedures.

[21/] In March 2007 and March 2008, OIG reported on FBI Section 215 use in 2002-2006. OIG identified no illegal use of the authority, but reported four instances of overproduction resulting from inadvertence or telephone company error. OIG is scheduled to review Section 215 use in 2007-2009 as well as actions in response to its recommendation that the Attorney General adopt minimization procedures for Section 215 information (which has not yet occurred).

4. Recommendation

Based on the FBI's operational experience and given these safeguards, we believe that Section 215 should remain in effect. FBI national security investigators need the ability to obtain records that are outside the scope of the NSL statutes when working in an environment that precludes the use of less secure criminal authorities. Moreover, criminal authorities may be unavailable when an investigation is not focused on a violation of criminal law. As in the past, many requests will be mundane, such as seeking driver's license information that state law protects from disclosure. Other requests will be more complex, such as the need to track the activities of targets through their use of business services. The availability of the FISC-supervised business records authority is an appropriate way to advance national security investigations in a manner that protects civil liberties and privacy interests. The absence of this authority could force the FBI to sacrifice key intelligence opportunities, to the detriment of the national security.

To ensure that FBI policies and procedures are effective in minimizing the risk, OIC and the Inspection Division should regularly conduct, as experience indicates, compliance reviews and audits of the FBI's use of the Section 215 business records, adherence to Section 215 minimization procedures, and use of pen registers and trap-and-trace authority.

D. Roving Surveillance Authority

1. Background

The FBI's roving surveillance authority under FISA is an important intelligence-gathering tool in a small but significant subset of investigations. The authority is only available when the government provides the FISC with "specific facts" that the target may engage in activities that thwart the identification of communications service providers (such as rapidly switching mobile phone companies). See 50 U.S.C. § 1805(c)(2)(B). The authority is subject to FISA's touchstone evidentiary requirement: the government must demonstrate probable cause that the target is a foreign power or an agent of foreign power and that the target is using, or is about to use, a communications facility such as a telephone.

From 2001, when the roving surveillance authority was added to FISA, through 2010, the FISC has granted approximately [redacted] FBI requests to use this authority.

2. Concerns

Critics worry that this authority vests Agents with an inappropriate level of discretion and enables the FISC to issue surveillance orders that specify neither the person targeted nor the device to be monitored. They argue that FISA should be amended to require the order to identify either the device or individual being intercepted.

3. Evaluation

A roving intercept may be critical to effective national security surveillance. Agents have observed targets of FISA surveillance engage in counter-surveillance and instruct associates on

how to communicate through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards).

FISA requires the FBI to describe the target of roving surveillance with particularity and to report to the FISC within ten days (or more, if the Court permits) of using roving surveillance authority on a new communications device. The report must state, among other details: (1) the facts and circumstances supporting the FBI's belief that the target was using the device; and (2) how the FBI will adapt standard minimization procedures to limit the acquisition, retention, and dissemination of communications involving U.S. persons that might be collected. 50 U.S.C. § 1805(c)(3).

We believe that this reporting requirement refutes the suggestion that the Title III ascertainment requirement should be imported into FISA. Adding a requirement that the government know that the target is proximate to the facility would effectively require the FBI to maintain constant physical surveillance of the target or risk missing communications it is otherwise entitled to intercept. That risk is substantial when dealing with surveillance-conscious targets. The reporting requirement guards against misuse of the authority. There have been no known major compliance issues with grants of roving surveillance authority.

We believe that the statutory safeguards provide for an appropriate balance between the FBI's national security needs and privacy rights and civil liberties. We also believe that the justification for the roving surveillance authority offered to Congress in 2001 remains valid today. The technological advances of the past decade have only heightened its importance. The FBI is confronted with the increased availability of prepaid (throw-away) mobile phones; the ease of adding and/or porting telephone numbers; easily established email and messaging accounts; and other readily accessible means of electronic communications. As these widely-available and often-free technologies develop and diversify, the need for roving surveillance authority to help protect national security will continue to grow.

4. Recommendation

In light of the FISA legal threshold and judicial oversight of the exercise of the roving surveillance authority, we believe this essential tool for protecting national security should remain in effect. We believe that the judicial oversight required by FISA is sufficient to ensure that the authority is used as intended.

E. "Lone Wolf" Authority

1. Background

The FISA "lone wolf" authority applies only to non-U.S. persons who "engage[] in international terrorism or activities in preparation therefor." See 50 U.S.C. §§ 1801(i) and 1801(b)(2)(C). The government must otherwise satisfy the requirements of FISA, including the requirement of certification that a significant purpose of the surveillance is to collect foreign intelligence information. In practice, this means that the government will likely know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to

satisfy the definition of "international terrorism"), but may not be able to connect the individual to a group that meets the FISA definition of a foreign power.

2. Concerns

Critics contend that, because terrorism is a crime, the government could obtain a Title III surveillance order from a criminal court if there is probable cause to believe that a lone individual is planning a terrorist act. They thus believe that there is no need for the authority. On the other hand, some non-FBI interviewees suggested that the statute should be expanded to include U.S. persons.

3. Evaluation

There are scenarios where this authority would provide the only avenue to effect surveillance of a foreign terrorist. A non-U.S. person could sever ties with a foreign terrorist group after an internal dispute, yet remain committed to international terrorism. In that event, absent this provision, the government may not be able to show probable cause to believe he is an agent of a foreign terrorist group and thus a permitted target of FISA surveillance. Without the "lone wolf" authority, the government could not initiate or could be forced to postpone FISA surveillance until the person could be linked to a foreign terrorist group – even though he posed a real and imminent threat. The "lone wolf" provision may also be needed to conduct surveillance of a non-U.S. person who "self-radicalizes" using inspiration, information, or training obtained on the Internet or through other means not connected to a foreign terrorist group. This non-U.S. person could adopt the aims and means of international terrorism without being a member of, or acting as an agent of, a terrorist group.

[redacted] The tool is thus essential for the rare situations in which investigators identify a non-U.S. person engaged in foreign terrorist activities, but cannot immediately connect that person to a foreign terrorist group. The narrow language of this provision minimizes the risk of overuse. To assure effective oversight, the FBI has committed to notify the appropriate Congressional committees if it invokes the authority. We believe that the authority should be preserved.

We do not believe, however, that the provision should be expanded to include U.S. persons. FBI counterterrorism personnel we interviewed saw no overriding operational reason for this change because Title III authority exists for electronic surveillance and physical searches of U.S. persons suspected of terrorist activities. Title III surveillance may not be as efficient and effective as FISA surveillance in counterterrorism investigations, but we believe that the use of Title III is a better balance of the competing interests when a U.S. person is involved. Moreover, because FISA's primary purpose is to acquire foreign intelligence, the absence of an established foreign connection could raise serious legal issues if the target were a U.S. person engaged in criminal activities.

4. Recommendation

We believe that the "lone wolf" authority as enacted should remain in effect and that the judicial oversight required by FISA is sufficient to ensure that the authority is used as intended.

Additional Authorities

The Terms of Reference also asked Judge Webster to "review ... whether the FBI should propose any legislative action to improve its ability to deter and detect such threats [as those posed by Major Hasan] while still respecting privacy and civil liberty interests."

We interviewed a broad range of FBI personnel involved in counterterrorism work at Headquarters and in the field; 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 for legislative action, we identified two in particular that the FBI has proposed or could propose to improve its ability to deter and detect terrorist threats: amendments to the Communications Assistance for Law Enforcement Act (CALEA)(1994), 47 U.S.C. § 1001 et seq., and definitive and consistent counterterrorism administrative subpoena authority. The FBI believes, and we agree, that amending CALEA is an immediate priority.

A. CALEA in the Twenty-First Century: "Going Dark"

1. Background

Our investigation revealed the adverse impact of evolving technologies on the FBI's lawfully authorized ability to access, collect, and intercept real-time and stored communications. Since the passage of the CALEA in 1994, electronic communications technologies have evolved in diverse and dramatic ways. New and popular modes of electronic communications – text, voice, and video – exist and flourish outside the scope of CALEA, challenging the FBI's practical ability to conduct timely and effective lawful electronic surveillance of communications by terrorists and other criminal threats to public safety and national security.

The FBI is confronted by the likelihood that any given subject of an assessment or investigation will have access to multiple communications devices, service providers, accounts, and access points. Nidal Hasan possessed or had access to a mobile telephone, a pager, four computers, three private email accounts with two service providers, five military email accounts, and access points ranging from his apartment to his workplace, as well as any merchant or municipality that provided a WiFi hotspot.

There is no known evidence that Hasan used any form of electronic communication other than website posts and email to attempt to contact Aulaqi (see Chapters 5 and 6). However, our investigation disclosed that Aulaqi [and others had] [redacted] exploited [electronic communications technology] [redacted] in an effort to conceal their identities, geographic locations, and operational activities. The same problem exists in criminal contexts, notably in child exploitation/pornography contexts and drug trafficking.

The use of advanced technologies by terrorists and criminals is worrisome because of the FBI's increasing inability to intercept communications using those technologies. When CALEA was enacted in 1994, a handful of large companies serviced most U.S. telephone users using relatively standard technologies. CALEA sought to maintain law enforcement's ability to conduct surveillance of communications services using traditional land line and cellular platforms. In 2005, the Federal Communications Commission (FCC) applied CALEA to "interconnected" VoIP services and providers of facilities-based broadband access services. At that time, there were nearly 40 million high-speed Internet lines serving U.S. residences and businesses, and at least one high-speed provider in 95% of U.S. zip codes. See FCC News Release, *Federal Communications Commission Releases Data on High-Speed Services for Internet Access* (July 7, 2005).

CALEA does not apply, however, to other Internet-based or -enabled technologies, notably VoIP services that fall outside the FCC's definition of "interconnected" VoIP services (for example, one-way calling services, peer-to-peer communications services, and other voice communications services provided by Internet Service Providers). Although many U.S.-based service providers not subject to CALEA cooperate with the FBI, they are not required to have, and do not all have or maintain, the capability to enable prompt and effective surveillance of their communication services.

The FBI refers to the impact of the widening gap in its ability to conduct lawful electronic surveillance as "Going Dark." E.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing before the H. Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (2011) (statement of then-FBI General Counsel Valerie Caproni). We believe that the FBI should pursue legislation that will bring communications assistance to the FBI and other law enforcement agencies into the Twenty-First Century.

The electronic communications revolution is global. An increasing number of enterprises have facilities outside the U.S. that provide services to persons in the U.S., which creates significant jurisdictional, logistical, and technical complexities for conducting lawful electronic surveillance on their facilities. Modernizing the scope of the requirement to have lawful intercept capabilities would not be effective unless the FBI also had access to off-shore enterprises that provide services inside the U.S. The FBI thus believes it is important to require communications service providers to U.S persons to maintain an operational "point-of-presence" in the U.S. for the conduct of electronic surveillance.

2. Concerns

Any proposal to amend CALEA must consider the potential impact on the civil liberties and privacy interests of U.S. persons, as well as the compliance costs placed on private enterprise. E.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,* Hearing before the H. Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (2011) (Statement of Laura W. Murphy, Director, Washington Legislative Office, ACLU). The ACLU has expressed a primary concern about the potential for limitless reach inherent in any proposal to regulate electronic communications providers in an increasingly interconnected and Internet-reliant world. There is also concern that the costs of fulfilling CALEA's capability and capacity requirements will be passed through to consumers and could inhibit the development of new and

innovative technologies. For these reasons, the ACLU concludes that CALEA should not be extended to communications methods unless the FBI and other law enforcement agencies demonstrate an associated threat to the U.S.

These are important concerns. Congress enacted CALEA to assure that law enforcement obtains prompt and effective access to communications services when conducting a lawful electronic surveillance during the investigation of a threat. The statute is founded on the recognition that lawful electronic surveillance activities may be difficult, if not impossible, absent an existing level of capability and capacity on the part of communications service providers. New communications technologies do not pose a threat to the U.S. The threat to our national security – implicit in CALEA and increasingly explicit in FBI investigations – is the lack of surveillance capability and capacity on the part of service providers that use those new technologies. The FBI's proposed amendments would require those service providers to fulfill the same capability and capacity requirements that the telecommunications industry has fulfilled for nearly 20 years.

3. Recommendation

In view of the weighty impact of evolving technologies on FBI intelligence-gathering and counterterrorism operations, the FBI should pursue its proposed amendments to CALEA. In considering those proposals, Congress should weigh the FBI's operational needs and the specter of "going dark" with the potential effects on privacy rights and civil liberties.

B. Counterterrorism Administrative Subpoena Authority

1. Background

The FBI's counterterrorism authorities are not as robust 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. Because counterterrorism is the government's highest national security priority, 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.

Proposals have been advanced to authorize the FBI to issue administrative subpoenas to compel the production of records and documents in aid of terrorism investigations. Some proposals would also authorize the FBI to compel testimony. Others would replace the NSL statutes with administrative subpoena authority in order to simplify and streamline the law.[22/]

One notable proposal we received would authorize the FBI to secure third-party records – but not testimony – modeled on 21 U.S.C. § 876, which authorizes DOJ agencies to issue subpoenas for records relevant to narcotics investigations. The proposal would apply only in terrorism investigations, not in other national security investigations. It would not be available to obtain those sensitive records identified in FISA Section 215 (library circulation records and patron lists, book sales records, book customer lists, firearms sales records, tax return records, and educational records and medical records containing information that would identify a person). Agents seeking those records would have to use Section 215. Finally, the proposal would adopt Section 215 and NSL safeguards, including the internal approval requirements and the mechanisms for challenging the subpoena and any non-disclosure order.

Proponents of FBI counterterrorism administrative subpoena authority, including Special Agents we interviewed in the field, believe that time is often of the essence in terrorism investigations, and the FBI should have the ability lawfully to compel third parties to provide

---

[22/] For example, in April 2008, David Kris, former Assistant Attorney General, DOJ National Security Division, but at that time a private citizen, proposed legislation in testimony before the Subcommittee on the Constitution, Civil Rights and Civil Liberties of the House Committee on the Judiciary that would enact "a single statute, providing for national security subpoenas, to replace all of the current NSL provisions." *National Security Letters Reform Act of 2007: Hearing on H.R. 3189 Before the H. Subcomm. on the Constitution, Civil Rights and Civil Liberties*, 110th Cong. (2008) (statement of David Kris), at 1. Mr. Kris stated that any new statute should satisfy ten essential elements described in his written submission – most notably, that national security subpoenas should be (1) issued by DOJ lawyers; (2) limited to acquiring specified types of foreign intelligence or other protective information; and (3) governed by rigorous minimization procedures concerning acquisition, retention, and dissemination of information. Id. at 2; see also Christophir Kerr, *What the Real Jack Bauers Really Need: A New Subpoena*, 1 William & Mary Policy Rev. 51 (2010), in which a former FBI Agent, proposes national security subpoena authority for the FBI similar to grand jury and other administrative subpoenas, with high-level approval required for subpoenas of organizations engaged in First Amendment political advocacy and with independent judicial review.

information as quickly as possible. It is not difficult to imagine an urgent scenario in which obtaining a grand jury subpoena for documents from a federal prosecutor is not practicable. Assume, for example, that Top Secret, compartmentalized information suggests that the FBI should obtain certain records from a chemical supply company. To obtain a grand jury subpoena for those records, the Agent would need to describe the underlying information to allow the AUSA to determine whether the records are relevant. That would require access to an AUSA with a Top Secret security clearance who has been "read in" to the relevant compartment. At night and on weekends, even if such an AUSA was available, establishing a secure method of communication could be difficult, if not logistically impossible. Moreover, there is no general legal requirement that recipients of grand jury subpoenas keep them secret, further complicating reliance on the grand jury as a method of compelling production of documents. See also Testimony of Rachel Brand, Principal Dep. Asst. Attorney General, Office of Legal Policy, before the Subcomm. on Terrorism, Technology and Homeland Security of the Senate Judiciary Comm. (June 22, 2004), at 6-7.

Proponents also say that the varying procedural and substantive standards in the NSL statutes create practical difficulties in the field. The OIG 2008 NSL report revealed, for example, that FBI agents did not always appreciate the difference between NSLs under 15 U.S.C. §§ 1681u and 1681v of the Fair Credit Reporting Act. The result was that agents were sometimes slow to use the NSLs and sometimes used them incorrectly – to the potential detriment of both national security and civil liberties.

Proponents acknowledge that the FBI mishandled its expanded NSL authorities in the wake of 9/11 – as described in the DOJ Inspector General's 2007 report – but argue that these problems were resolved by the expansion of FBI and National Security Division oversight and the implementation of an effective NSL subsystem to ensure that all statutory and regulatory requirements are satisfied before an NSL may be issued. These same measures, proponents say, would apply to any broader administrative subpoena authority and prevent that new authority from succumbing to the problems revealed by the Inspector General's report.

2. Concerns

Opponents argue that administrative subpoena authority in terrorism cases would fundamentally change the traditional limits on law enforcement interference with privacy rights and civil liberties. They cite important checks and balances on the government's authority to compel the production of documents and express concern that administrative subpoenas would compel U.S. citizens to produce documents, potentially in secret on certification by the Attorney General, without the participation or protection of a U.S. Attorney, grand jury, or judge. No showing of reasonable suspicion, probable cause, or even imminent need or exigent circumstances would be required. That is true, however, about administrative subpoenas in any context, as issued by any number of other federal departments and agencies.

Opponents recognize that the swift production of documents can be critical to the FBI's ability to prevent terrorist acts. They note, however, that the administrative subpoena proposals do not require an imminent threat of harm. They suggest alternative ways to obtain the immediate production of documents: amending FISA to provide for emergency Section 215 orders; posting "duty" AUSAs to be available around the clock for issuing grand jury subpoenas;

and/or limiting administrative subpoena authority to exigent circumstances as certified by the FBI Director (similar to the Secret Service Director's authority to issue administrative subpoenas under 18 U.S.C. § 3486(a)(1)(A)(ii) in the event of an imminent threat of harm to a protectee). They also note that secrecy can be achieved by providing for non-disclosure of counterterrorism grand jury subpoenas upon certification of need.

At hearings held by the Subcommittee on Terrorism, Technology and Homeland Security of the Senate Judiciary Committee in 2004, the principal justifications advanced by DOJ and other witnesses (as well as Senators) for administrative subpoena authority were the need for speed and the risk that an AUSA would not be available. However, in a response to a written question from Senator Patrick Leahy in January 2005, DOJ stated that it was "unaware of any specific instances in which an AUSA's inability to sign off on an emergency grand jury subpoena resulted in a loss of evidence or some other irrevocable consequences [to] a pending investigation." A Review of the Tools to Fight Terrorism Act: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary, 108th Cong., 2d Sess. (2004), at 38. Proponents argue, nonetheless, that the absence of this tool naturally slows or disrupts investigations. When a terrorism investigation must resort to a more cumbersome or time-consuming tool because the NSL statutes do not reach the needed information, real or potential terrorists might gain an advantage.

3. Recommendation

Given the FBI's view that administrative subpoena authority for terrorism investigations would be useful in potentially critical situations and in resolving the complexities of the NSL statutes, the FBI could seek a definitive and consistent administrative subpoena authority that is compatible with its counterterrorism mission. If this authority is sought, then Congress should weigh the FBI's operational needs against the potential effects on privacy rights and civil liberties. We recommend consideration of the following salient issues:

- Consistency: Should the FBI have the authority to issue administrative subpoenas in narcotics and child pornography investigations, but not in terrorism investigations?

- Need: Have the proponents of counterterrorism administrative subpoena authority justified its operational need or usefulness? Although the government has not cited instances when the lack of this authority resulted in lost evidence or harm, other justifications (such as the elimination of confusion and complexity) exist. Are there alternative authorities that would meet the government's needs (such as emergency Section 215 orders or Director certified subpoenas in exigent circumstances)?

- Availability and Scope: Should, as suggested by some non-FBI commenters, the use of the subpoenas be available in assessments, or should they be available only in predicated investigations? Should the subpoenas reach all records, or should Section 215 "sensitive" documents be excluded? Should the subpoenas compel testimony as well as documents and records?

- Issuer: Should the FBI have the authority to issue the subpoenas (as it does with NSLs and other administrative subpoenas) or should a DOJ attorney (for example, an AUSA) issue them as is done with grand jury subpoenas?

- Standard: Should the subpoenas issue based on "relevance to an authorized investigation" or a standard that requires a closer nexus to and/or predicate for the investigation?

- Non-Disclosure/Secrecy: Should the non-disclosure and judicial review provisions of the NSL statutes (as modified to reflect Doe v. Mukasey) govern the subpoenas?

- Minimization: What minimization procedures, if any, should apply to the acquisition, retention, and dissemination of records acquired by the subpoenas?

- Reports/Audits: Should counterterrorism administrative subpoena authority include required reporting to Congress, OIG and National Security Division audits, and/or FBI OIC compliance reviews and Inspection Division audits?

Congress is responsible for assessing these issues and determining whether to grant the FBI administrative subpoena authority for terrorism investigations. We offer the following thoughts.

First, whether or not subpoena authority is granted, the varied standards of the NSL statutes should be reconciled and made consistent.

Second, if the authority is granted, the FBI should adopt and implement strict document access and control protocols to ensure that acquired information that lacks current investigative value is not improperly accessed, retained, or disseminated. Those protocols would be comparable to those the FBI is implementing to limit dissemination of certain NSL information or to the restricted access that is provided for grand jury material.

Third, any counterterrorism administrative subpoena authority should be subject to oversight by Congress, OIG, and NSD. Initially, this should include periodic reports to Congress as experience indicates and annual OIG/NSD audits. The FBI's OIC should be tasked with lead responsibility for identifying potential compliance risks, devise and monitor measures to mitigate those risks, and coordinate with the FBI Inspection Division to conduct compliance reviews and audits. The FBI should also expand the NSL subsystem to include any subpoena authority to ensure that the appropriate authority is invoked, that all required approvals (including legal review) are obtained, and that the relevant investigative file has been opened in accordance with the AG Guidelines.

A 2008 Inspection Division review of the FBI's use of existing administrative subpoena authorities found that the process for obtaining these subpoenas allowed Agents to use them for investigations not authorized by statute in five percent of sampled cases. (The overall non-compliance rate was higher for all compliance issues, including administrative errors such as missing or incorrect citations.) The review also found that the FBI lacked a standardized mechanism to track the number of administrative subpoenas issued. To mitigate non-compliance

risks, ICP developed a plan to automate the process for issuing administrative subpoenas. A March 2011 Inspection Division audit found, however, that compliance concerns remained, and recommended further mitigation of compliance risks. The ICP has developed a corrective action plan. The FBI should ensure that any steps taken under that plan would apply to any counterterrorism administrative subpoena authority.

Part Five

Recommendations

The Terms of Reference asked Judge Webster to assess "whether there are other policy or procedural steps the FBI should consider to improve its ability to detect and deter ... threats such as that posed by Major Hasan ... while still respecting privacy and civil-liberty interests" and "whether any administrative action should be taken against any employee."

We make eighteen recommendations for policy, procedural, and other actions to be taken by the FBI and/or the Attorney General. We then discuss the conclusions of our careful deliberations about whether administrative action should be taken against any employee.

We recognize that the FBI has continued to evolve as an intelligence and law enforcement agency in the aftermath of the Fort Hood shootings 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. We understand, for example, that the FBI has drafted written policies that would fulfill our Recommendations A.1, A.6, and A.7 below. We urge the FBI to finalize and promulgate these policies.

A. POLICIES

RECOMMENDATION A.1:

A Formal Policy on Counterterrorism Command-and-Control Hierarchy

The FBI should prepare and promulgate a written policy that identifies the division of authority and the command-and-control hierarchy among the FBI's Headquarters entities (including the Counterterrorism Division, NJTTF, and the Directorate of Intelligence) and its field entities (including Field Offices and JTTFs). The policy should provide a clear understanding of each entity's responsibility, authority, and accountability within the FBI and in interactions with other governmental departments and agencies.

RECOMMENDATION A.2:

A Formal Policy on the Ownership of Counterterrorism Leads

The FBI should prepare and promulgate a written policy establishing ownership and ultimate responsibility when one Field Office or JTTF sets a counterterrorism lead to another Field Office or JTTF. This policy should adopt current FBI practice that the receiving office has ultimate responsibility for resolving leads set by other Field Offices or JTTFs. This policy should also discuss procedures for resolving disagreements between Field Offices, JTTFs, and other FBI entities.

The FBI should also consider applying this policy to national security, criminal, and other investigative contexts.

RECOMMENDATION A.3:

A Formal Policy on Elevated Review of Interoffice Disagreements in Counterterrorism Contexts

The FBI should prepare and promulgate, either alone or in the context of Recommendations A.1 and A.2, written policy identifying the procedures for resolving inter-office disagreements in counterterrorism contexts, whether about the adequacy of a response to a lead or any other subject. We recommend that the FBI adopt the existing informal process of elevating disagreements up the chain-of-command within Field Offices and JTTFs (Special Agent-Supervisory Special Agent-Assistant Special Agent in Charge-Special Agent in Charge). We recommend that the policy identify when and how to contact FBI Headquarters; who should be contacted at FBI Headquarters; and who should become involved in the resolution of disagreements. We also recommend that the FBI train all personnel on the elevation of interoffice disagreements.

The FBI should also consider applying this policy to national security, criminal, and other investigative contexts.

RECOMMENDATION A.4:

A Formal Policy on the Assignment and Completion of Routine Counterterrorism Leads

The FBI should prepare and promulgate a written policy for prioritizing Routine counterterrorism leads set outside of the Guardian system. This policy should adopt reasonable deadlines for the assignment of Routine leads and for responses to these leads. As our investigation revealed, formal deadlines will assure that supervisors and assignees read and handle leads in a timely manner. Nearly fifty days passed before the supervisor read and assigned the Hasan lead. Another ninety days passed before the assignee read and took action on the lead.

Our investigation also revealed, however, that mere adherence to deadlines is not necessarily consistent with effectiveness. By allowing the assignee to wait until the ninetieth day – the deadline for response under informal FBI practice – to read and take action on the lead, WFO denied itself the time to conduct a thoughtful and adequate assessment. Expediting assessments and preliminary investigations by imposing tight deadlines would likewise risk denying the Agent, Analyst, or Task Force Officer time to provide a thoughtful and complete response. We are also concerned about the imposition of unreasonable deadlines on personnel who are already working heavy caseloads with varied and constant demands on their time.

The FBI's published Guardian Policy and System Guidelines, which apply to Type 1 and 2 assessments, require supervisors to ensure that Routine incidents are assigned within five business days and state that "[e]very attempt must be made to 'mitigate' Guardian incidents within the first 30 days." [redacted] [FBI policy number

redacted]. The 30-day period can be extended if the supervisor provides a documented justification. Compliance with these deadlines is monitored and audited by a Headquarters unit, the Assessment Review Team.

We recommend that the FBI policy on prioritizing Routine non-Guardian leads in counterterrorism contexts should (1) require the receiving supervisor to assign the lead within, at minimum, two weeks of receipt; (2) adopt the existing informal practice that work on a lead must be completed within 90 days of assignment (unless the supervisor imposes a shorter deadline); and (3) provide for Headquarters-level monitoring and audits of compliance with these deadlines through the ITOS unit responsible for program management of the relevant Field Office or JTTF. The policy should provide for an extension of the 90-day deadline if the assignee provides written evidence to his or her supervisor that circumstances such as the exceptional demands of the lead or workload render it unreasonable to complete the work within 90 days. We also expect the FBI to establish and enforce robust management and monitoring procedures to assure that inexcusable delays of the type that occurred in the Hasan matter do not recur.

RECOMMENDATION A.5:

A Formal Policy on Counterterrorism Leads Assigned to JTTF Task Force Officers

The FBI should prepare and promulgate a written policy that no JTTF Task Force Officer will be assigned lead responsibility for an assessment or investigation of an employee of his or her home department, agency, or authority. We encourage reliance on Task Force Officers as consultants in these contexts; but the FBI is ultimately responsible for the activities of its JTTFs, and its Special Agents are best prepared and best qualified to conduct counterterrorism investigations – as citizens, we want the FBI to investigate in these contexts. As a result, FBI Special Agents should take lead responsibility for conducting any assessment or investigation of an employee of a department, agency, or authority that has provided a Task Force Officer to the relevant JTTF.

RECOMMENDATION A.6:

A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessments and Investigations of Law Enforcement Personnel

Although the military context of the Fort Hood shootings has focused attention on information-sharing and other measures involving the Department of Defense, we believe that equal, if not potentially greater, national security risks could arise in other contexts involving government employees with ready access to weapons and intelligence. We recommend that the FBI finalize and promulgate a written policy requiring Field Offices and JTTFs to notify the Counterterrorism Division – which will, in turn, advise the NJTTF – of any counterterrorism assessment or investigation of a known member of a federal, state, local, or tribal law enforcement agency. Under this policy, the NJTTF's Homeland Security component should track these assessments and investigations, while the Counterterrorism Division should determine whether the subject's agency can and should be notified of the

assessment/investigation or its predication. Any disclosure would comply with FISA minimization procedures. This policy would parallel the FBI-DoD clearinghouse procedure in assuring that Field Offices and JTTFs provide timely and consistent notice of counterterrorism assessments and investigations of law enforcement personnel to the NJTTF and, if appropriate, to the law enforcement agency involved.

RECOMMENDATION A.7:

A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessments and Investigations of Other Government Personnel

We do not believe that the FBI-DoD clearinghouse procedure and the policy proposed by Recommendation A.6 are sufficient to resolve the information-sharing risks implicated by the Hasan matter. We recommend that the FBI identify other federal departments and agencies outside military and law enforcement contexts (for example, the Department of State and the Transportation Security Administration) as subjects of comparable information-sharing procedures. We recommend that the FBI then finalize and promulgate a written policy requiring Field Offices and JTTFs to inform the Counterterrorism Division and the NJTTF of counterterrorism assessments and investigations involving employees of those departments and agencies. This policy should place responsibility on the Counterterrorism Division to determine whether to disclose the assessment or investigation to the relevant department or agency. Any disclosure should comply with FISA minimization procedures.

B. OPERATIONS

RECOMMENDATION B.1:

Continued Integration of Intelligence Analysts into Operations

Throughout our investigation, we were impressed by the quality and commitment of the FBI's Intelligence Analysts – and by the increasingly effective integration of those Intelligence Analysts into the FBI's hierarchy and culture. The FBI has made notable progress in embedding Intelligence Analysts in the Counterterrorism Division and the Counterterrorism Analysis Section in operational squads, in implementing counterterrorism "fusion cells," and in pursuing initiatives to apply the "fusion cell" model across its operational divisions. We recommend that the FBI continue to increase the number and participation of Intelligence Analysts in its operational divisions.

C. INFORMATION TECHNOLOGY AND REVIEW

Our investigation witnessed, first-hand, the impact of the ever-increasing diversity and complexity of communications technologies and services – and the ever-expanding amount of electronically stored information – on the FBI's electronic surveillance and information review and management capabilities. The FBI and other law enforcement agencies need the financial

resources, capability mandates, and human and technological capacity to respond to these complex and sensitive issues.

The ability to conduct effective electronic surveillance in the face of evolving technologies and massive accumulations of data represents only half of the challenge. The ability to acquire and collect information is meaningless unless the FBI has the technology, the human resources, and the protocols to review, analyze, relate, manage, and act on that information in a timely and effective manner. On January 7, 2010, two months after the Fort Hood shootings, the President issued a directive to the U.S. Intelligence Community to "[a]ccelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence." We concur fully with that directive.

Our Technology Recommendations have financial implications in a time of budgetary constraints. To the extent these Recommendations would require the FBI to divert funding from projects of equal or greater importance or from system maintenance, we urge the FBI to seek additional funding for what we believe to be crucial technology needs.

RECOMMENDATION C.1:

Expedite Enterprise Data Management Projects

The historical evolution of the [multiple] FBI [redacted] [and other U.S. Intelligence Community (USIC)] databases as discrete platforms has impeded the FBI [and USIC's] ability to access, search, organize, and manage electronically stored information [in an efficient manner].

[redacted]

Because information is the FBI's essential tool as an intelligence and law enforcement agency, we recommend that the FBI expedite and, if appropriate, seek expanded funding for Enterprise Data Management projects, with an initial emphasis on aggregation of its primary investigative databases, the collection and storage of data as a service separate from applications, and the development of shared storage solutions across USIC members.

Enterprise Data Management is the process of normalizing, consolidating, integrating, and federating information technology platforms, systems, and data to increase consistency and efficiency in storage, search, management and, when possible, sharing of data holdings. In the ideal, Enterprise Data Management projects would resolve FBI databases into a handful, at most, of access-controlled databases that could be reviewed using common search and management

tools while also pursuing access-controlled interagency solutions to the collection and sharing of information without copying across agencies. In most public and private enterprises, budget considerations require Enterprise Data Management to occur only as and when specific platforms and systems are replaced or removed from service. Because data is now the FBI's primary business, Enterprise Data Management cannot wait, and should be addressed immediately as an essential priority.

RECOMMENDATION C.2:

Expand and Enhance the Data Integration and Visualization System

In January 2010, as a first step in responding to the President's directive on information technology enhancements, Director Mueller tasked the Special Technologies & Applications Section (STAS) with developing a means of searching across the FBI's primary repositories of data. The result, deployed in October 2010, is the Data Integration and Visualization System (DIVS).

DIVS provides a one-password, access-controlled, integrated search capability that allows Agents, Analysts, TFOs, Linguists, Language Support Specialists, and Staff Operations Specialists to conduct searches across FBI data stores that otherwise do not and cannot connect with each other. Its Google-like interface returns results from each database that the user is authorized to access (and reports any results that exist on databases the user does not have authority to access).

At this writing, DIVS provides users with the ability to search across [more than fifty FBI and non-FBI] databases STAS plans to expand the reach of DIVS to other [FBI and] U.S. Intelligence Community, law enforcement, and public data sets.

Although DIVS is a visually appealing and impressive search tool, it is a short-term and somewhat superficial solution to the FBI's proliferation of databases. It is crucial that FBI management understand that DIVS, in its existing design, is only an indexing and search tool. DIVS does not aggregate or convert data; instead, it creates and searches a massive index of the content of the included databases. When the user selects a return for review, DIVS opens that file in its native database application; thus, for example, if a search returns a result from DWS-EDMS, a click on that result will take the user to that item in DWS-EDMS. The user then conducts review and further searches of that item in DWS-EDMS.

DIVS does not and cannot normalize and consolidate the FBI's balkanized data stores or otherwise provide true interconnectivity of databases. Its search capabilities are welcome, but

should not be interpreted as anything but a bridge to the essential solution of an Enterprise Data Aggregation Plan.

RECOMMENDATION C.3:

Acquire Modern and Expanded Hardware for DWS-EDMS

The limited functionality of DIVS also underscores the importance of the individual systems that house the FBI's primary databases and the need to assure that those systems are robust, reliable, and sustainable. DIVS is only as good as the databases it indexes and searches. The addition of its cross-database search capability should not cause the FBI to lose focus on DWS-EDMS, whose functionality cannot be replicated or replaced by DIVS.

Although originally designed by the Special Technologies & Applications Section (STAS) as a transactional warehouse, DWS-EDMS has evolved, through STAS's expertise, into one of the FBI's workhorse systems. [redacted] The [September] 2011 [redacted] enhancement provided a more intuitive user experience, automation of tasks, and a significant increase in reviewer efficiency and accuracy.

When our investigation began, some hardware components of DWS-EDMS were eight years old and stressed. During the course of our investigation, STAS migrated DWS-EDMS to a new generation of hardware. The design of the new DWS-EDMS system permits the addition of equipment as needed, thus allowing STAS to maintain system performance at an acceptable operational standard.

Our investigation also disclosed that DWS-EDMS is operating without a "live" disaster recovery backup system. [redacted] We believe Congress should provide the FBI with funding for additional system investments.

We recommend that the FBI seek funding for the immediate acquisition of new hardware for DWS-EDMS by no later than 2012. This hardware, which would house the database, website, and search and analysis software, as well as integration and development tools, will significantly enhance search, analysis, management, and authorized data mining functions. This upgrade should fulfill the likely data capacity requirements for DWS-EDMS through 2018. It would require no software development, but simply the acquisition of the following or similar hardware, which we identify as a matter of example only – the FBI will need to assess, validate, and update any potential system depending on its needs, and broader Intelligence Community initiatives, at

the time of implementation. The important point is that the FBI needs to pursue a system solution for the horizontal scaling of data. Based on technology existing at the time of our investigation, the following is an example of the hardware needs of DWS-EDMS in its current architecture:

Production System:

Integration/Development System:

[The redacted portions involve details of sensitive FBI information system capabilities and requirements.]

The Integration/Development System will also provide the FBI with an essential "live" or "failover" disaster recovery backup, although it would operate at a significantly reduced response rate, slowing searches and other activities. Given the crucial role that DWS-EDMS plays in counterterrorism and law enforcement activities, the optimum disaster recovery system would include a co-located duplicate of the Production System, enabling immediate replacement of the Production System in the event of disaster without any impact on system performance. We recommend that the FBI carefully assess the risks associated with operating only with the Integration/Development System as a disaster recovery backup and consider seeking funding from Congress for acquisition of a duplicate of the Production System for disaster recovery purposes – to continue with the example provided above, based on existing technology and architecture.

Optional "Live" Disaster Recovery Backup System:

[The redacted portion involves details of sensitive FBI information system capabilities and requirements.]

RECOMMENDATION C.4:

Acquire Advanced Information Search, Filtering, Retrieval, and Management Technologies

We recommend that the FBI evaluate and, if appropriate, acquire and implement advanced and automated search, filtering, retrieval, and management technologies to assist Agents, Analysts, TFOs, and other personnel in reviewing and managing data – particularly the contents of Strategic Collections [redacted]. These tools are an important means by which the FBI can hope to master the ever-expanding amount of electronic data in its possession.

Advanced search tools transcend the simplistic keyword searching and filtering available on most FBI databases by revealing communication patterns, compiling threads of electronic conversations, identifying near-duplicate documents, and performing other functions to narrow large data sets and focus review time on materials of potential significance. The most advanced search tool is "concept search" – sometimes called "analytics" – which dramatically enhances the volume, speed, and accuracy of human review.

Concept search tools use computational analysis of electronic information rather than keywords to produce their results. With keywords, the reviewer seeks out words that messages happen to share. Concept search tools, on the other hand, automatically analyze the language in electronic documents and link messages that contain the same or similar meanings. For example, a keyword search for "newspaper reporters" will return only messages that contain those words, while a concept search would identify and relate a message about newspaper reporters to a message about journalism even though the second message did not contain the words "newspaper" or "reporter." If the user identifies a few key documents at the outset, he or she can find and follow a path of related documents, including emails written by the same person using two different accounts.

Concept search tools are comparable to one of the FBI's standard tools, the Integrated Automated Fingerprint Identification System (IAFIS) (see C. Ball, *Clinching the Concept of Concept Search*, 2010). IAFIS, which is being replaced incrementally by the biometric Next Generation Identification System, compares a fingerprint found in the field to a database of more than 68 million known fingerprints. The system does not compare every aspect of a submitted print; instead, computer algorithms and/or fingerprint experts mark minute points, cores, and deltas as detected. The system compares the resulting digital geometric analysis of the ridges and bifurcations to its database of the geometric characteristics of known fingerprints. The system then returns a candidate list of potential matches.

IAFIS allows the FBI to narrow dramatically the universe of potential matches without considering every nuance of a fingerprint. To determine a true match, however, a human assesses the returns and decides whether the print is a match. IAFIS does not eliminate the need for human judgment, but assures a more efficient and effective use of FBI resources.

Applying a similar technique to email and other electronic documents, FBI personnel can use digital technology to analyze and compare texts instead of fingerprints. Imagine an alternative scenario in which Hasan used three different email accounts to communicate with Aulaqi without always using his name. A keyword search of DWS-EDMS using Hasan's name or one of the email addresses would not return all of the messages. A concept search based on the email messages from one account, however, would identify messages with similar characteristics and group them with a predicted percentage of similarity. Just as focusing on geometrically similar fingerprints speeds the matching of fingerprints, concept searching speeds human review of electronic documents and produces results that would not be possible using keyword searches.

Enabling a reviewer rapidly to relate and group similar documents reduces the risk of overlooking messages or mistakenly marking messages. Agents, Analysts, and TFOs would no longer assess [redacted] [communications] day-by-day, [redacted] [item-by-item,] but in the context of the entire [redacted] [collection] or of the many databases indexed by DIVS.

Technology-driven law firms and corporations have tested and implemented concept searching in civil and criminal cases. In one study, a team of six professional reviewers competed against a concept search engine in assessing the relevance of electronic documents to three issues. The human reviewers identified 51% of the relevant documents, with a low of 43% for one issue. The concept search engine identified more than 95% of the relevant documents, with a high of 98.8% for one issue. See Electronic Discovery Institute, 2009. In a 2009 test by Verizon, a concept search engine automatically identified responsive documents with an accuracy rate of 92%.

The FBI has implemented automated processes in the wake of the Fort Hood shootings [redacted] The FBI has also introduced automated [tools] to prioritize messages for review [redacted] Concept search tools, on the other hand, allow for far more accurate and efficient processes that would prioritize messages not only by [redacted] specified terms, but also by the content of messages and the relationship of that content to other messages and email addresses.

Concept search technology cannot and should not displace human review of DWS-EDMS and other FBI data stores; but it is an essential and inevitable tool. The FBI should place high priority on adopting and deploying this technology. We understand that the FBI recently completed a market survey of advanced analytic tools and has acquired analytic, collaboration, and knowledge management software.

RECOMMENDATION C.5:

Adopt Managed Information Review Protocols for Strategic Collections [redacted] and Other Large-Scale [Data Collections] [redacted]

We recommend that the FBI adopt and implement managed information review protocols for Strategic Collections [redacted] and other large-scale [redacted] [data collections]. These protocols should include:

(1) Training: Comprehensive, hands-on training on DWS-EDMS and, if appropriate, the target and the subject matter of the investigation.

(2) Project Management: A clear delineation of the roles and responsibilities of project managers and reviewers.

(3) Planning: A review plan tailored to the needs of the specific case.

(4) Mission-Specific Review Teams:
A case-specific review team assigned primary responsibility for (a) gathering investigative and operational intelligence; (b) [redacted] [reviewing and identifying information per FBI procedures]; (c) setting leads; (d) issuing case-specific Intelligence Information Reports; and (e) case development.
An analytical review team assigned primary responsibility for (a) gathering and assessing strategic intelligence; (b) analyzing that intelligence in the context of regional and other strategic intelligence; and (c) issuing strategic Intelligence Information Reports.

(5) Workflow: A well-designed procedure that encourages thoughtful, retrospective analysis of data as well as day-to-day reviewing and [redacted] [identifying] of products.

(6) Quality Control: A well-designed series of quality control measures that allow program management or the analytical review team to sample and test case-specific reviewer accuracy in [redacted] [identifying] and relating products – and to identify products requiring further review.

D. GOVERNING AUTHORITIES

RECOMMENDATION D.1:

Increase Office of Integrity and Compliance (OIC) and Inspection Division Compliance Reviews and Audits

We recommend that OIC and the Inspection Division conduct compliance reviews and audits on a regular basis as experience indicates is necessary to ensure FBI compliance with all policies applicable to assessments and all policies and procedures that guard against the inappropriate use of First Amendment activity or race, ethnicity, national origin, or religion as a basis for investigative activity and to identify any concern about or impact on privacy rights and civil liberties. The FBI – and, if necessary, Congress – should make available sufficient personnel and funds to ensure that effective compliance monitoring is achieved.

These audits and reviews should examine:

- The FBI's use of assessments and the investigative techniques authorized for use in assessments (at least annually for a period of three years).
- The FBI's collection, mapping, and other use of racial/ethnic demographics and behavioral characteristics.
- The efficacy of the Guardian Management Unit and the Assessment Review Team in ensuring that the FBI follows all DIOG and other policies, including those concerning the opening of assessments, the use of investigative techniques during assessments, and the retention of information collected during assessments in Guardian and other FBI databases.
- The FBI's use of undisclosed participation in counterterrorism investigations involving religious and other First Amendment organizations and self-radicalizing individuals.
- The FBI's use of undercover operations and activities, including the use of confidential human sources and undercover FBI employees, in counterterrorism investigations.
- The FBI's use of its National Security Letter, Section 215 Business Records, and pen register/trap-and-trace authority, and the efficacy of the FBI's NSL Procedures.
- The FBI's use of additional investigative techniques approved by DIOG 2.0.

Although we conclude that the AG Guidelines standard for opening an assessment and the available investigative techniques strike an appropriate balance, privacy rights and civil liberties may be implicated. The recommended compliance reviews should ensure that this balance holds and identify any concern about or impact on privacy rights or civil liberties. The guiding principle should be that, as the risk of potential infringement of individual privacy rights

and civil liberties increases, the level of factual predication, supervisory approval, and oversight should increase. The FBI should modify or abandon policies and protocols that experience proves to be unacceptably harmful to privacy rights or civil liberties.

RECOMMENDATION D.2:

Assure Strict Adherence to Policies That Ensure Security for Information That Lacks Current Investigative Value

The FBI should strictly adhere to existing policies to ensure that personnel are not accessing or viewing information that lacks current investigative value unless there is a legitimate law enforcement or intelligence reason, and that personnel observe the Privacy Act in retaining information concerning First Amendment activities.

The FBI should apply these policies with particular focus – and OIC monitoring – to information gathered during assessments that implicates privacy interests, civil liberties, or First Amendment or other Constitutional rights. This focus would supplement existing FBI policy that requires any investigative activity – including activity involving assemblies or associations of U.S. persons exercising their First Amendment rights – to have an authorized purpose under the AG Guidelines that is rationally related to the information sought and the technique to be employed.

RECOMMENDATION D.3:

The FBI's National Security Letter, Section 215 Business Record, Roving Wiretap, and "Lone Wolf" Authorities Should Remain in Effect

Based on the FBI's operational experience, we believe that the FBI's National Security Letter, Section 215 Business Record, Roving Wiretap, and "Lone Wolf" authorities are essential tools for protecting national security. The safeguards built into each authority, including minimization standards and judicial oversight, minimize risks to civil liberties and privacy interests. As noted in Recommendation D.1, OIC and Inspection Division review and audits of the FBI's use of NSL and Section 215 authorities will help ensure that balance is maintained between national security needs and privacy rights and civil liberties.

RECOMMENDATION D.4:

Update Attorney General Guidelines Affecting Extra-Territorial Operations

The Attorney General's Guidelines for Domestic Operations did not supersede those sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG) and the Attorney General's Guidelines for Extraterritorial FBI Operations that govern FBI activities in foreign territories. The NSIG has

not been updated since 2003. The Guidelines for Extraterritorial FBI Operations, which govern non-national security matters, have not been updated since 1993. Given the FBI's heightened intelligence requirements in combating terrorism and the need for clear guidance on operational matters, the FBI should continued to work with the Attorney General to update and, if possible, consolidate these guidelines with other Attorney General Guidelines.

E. TRAINING

RECOMMENDATION E.1:

Train Task Force Officers on FBI Databases Before They Join Joint Terrorism Task Forces

Under current FBI practice, new Joint Terrorism Task Force Officers must receive training on FBI databases relevant to their tasks within six months of obtaining access to FBI systems. As the Hasan matter underscores, TFO knowledge of and ability to use FBI databases can be crucial to an assessment or investigation. No TFO should be permitted to join a JTTF unless and until he or she has had adequate training on the FBI's primary investigative databases, including DWS-EDMS, DaLAS, Clearwater, and IDW, as well as the Automated Case System (ACS). We recommend that database training become a mandatory component of the TFO Orientation & Operations Course (JTOOC) at Quantico.

We recognize, however, that mandatory training requirements could create practical issues given the known complexities and delays in interagency transitions and security clearances. We thus recommend that the FBI require all Task Force Officers to complete basic JTTF training within sixty (60) days of joining a JTTF and that the FBI assure that Task Force Officers who have not completed basic JTTF training are not assigned leads or otherwise assigned primary responsibility for any investigative action.

F. ADMINISTRATIVE AND DISCIPLINARY ACTION

RECOMMENDATION F.1:

As the Terms of Reference requested, we carefully considered whether any administrative or disciplinary action should be taken against any FBI personnel. Although we are critical of certain actions and omissions, we do not regard any of those actions to be misconduct that would warrant administrative or disciplinary action. We believe administrative or disciplinary action would be appropriate if FBI personnel violated known written policies or other binding directives, or if FBI personnel obstructed our investigation or were not honest about their actions. None of the missteps described in this Report involved such misconduct. Indeed, some missteps occurred because there was no stated policy or binding directive in place that would have required different actions. For example, we believe the Washington Field Office took an unreasonably long time to read and respond to San Diego's lead, but absent formal policy guidance on the assignment and resolution of Routine leads, the delay cannot be said to involve misconduct. We therefore cannot and do not recommend any administrative or disciplinary action against any FBI personnel.

If the formal policies that we recommend in Section A above are adopted and implemented, they will provide not only guidance to FBI personnel, but also clear standards by which future actions of FBI personnel may be assessed.

We are not in a position to say – and therefore express no view about – whether any administrative action should be taken for performance-based reasons (as distinguished from misconduct). Performance appraisals of this kind must be made on the basis of comprehensive criteria and information beyond the scope of our investigation.

INDEX OF ACRONYMS

ACS	Automated Case Support
ACS-ECF	Automated Case Support – Electronic Case File
ACS-ICM	Automated Case Support – Investigative Case Management
ACS-UNI	Automated Case Support – Universal Index
AD	Assistant Director
ADIC	Assistant Director in Charge
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General's Guidelines for Domestic FBI Operations
AGG-Ext	Attorney General's Guidelines on Extraterritorial FBI Operations
AGG-UCO	Attorney General's Guidelines on FBI Undercover Operations
AOL	America OnLine
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
CART	Computer Analysis and Response Team
CALEA	Communications Assistance for Law Enforcement Act
CD	Counterintelligence Division
CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CONUS	Continental United States
CPO	Corporate Policy Office
CPU	Central Processing Unit
CSO	Chief Security Officer
CT-1	Counterterrorism Squad 1
CT-3	Counterterrorism Squad 3
CTD	Counterterrorism Division
CUORC	Criminal Undercover Operations Review Committee
DAD	Deputy Assistant Director
DaLAS	Data Loading and Analysis System
D.C.	District of Columbia
DCIS	Defense Criminal Investigative Service
DCO	Division Compliance Officer
DEIDS	Defense Employee Interactive Data System
DI	Directorate of Intelligence
DIOG	Domestic Investigations Operations Guide

DIVS	Data Integration and Visualization System
DMX	Digital Media Exploration Unit
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DWS	Data Warehouse System
DWS-EDMS	Data Warehouse System-Electronic Data Management System
EA	Emergency Authority
EAD	Executive Assistant Director
EC	Electronic Communication
ECAU	Electronic Communications Analysis Unit
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
EDI	Electronic Discovery Institute
ELSUR	Electronic Surveillance
EO	Executive Order
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINET	FBI Network
FCC	Federal Communications Commission
FCRA	Fair Credit Report Act
FGUSO	Field Guide for Undercover and Sensitive Operations
FI	Foreign Intelligence
FI	Full Investigation
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISAMS	FISA Management System
FISC	Foreign Intelligence Surveillance Court
FTTTF	FBI Foreign Terrorist Tracking Task Force
GC	General Counsel
GUI	Graphic User Interface
HIMU	Human Intelligence Management Unit
HR	House of Representatives
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Bureau of Immigration and Customs Enforcement
ICM	Investigative Case Management
IDW	Investigative Data Warehouse
IIR	Intelligence Information Report
ILB	FBI Investigative Law Branch
IOB	Intelligence Oversight Board

IP	Internet Protocol
IT	International Terrorism
ITOS	International Terrorism Operations Section
JTOOC	Joint Terrorism Task Force Officer Orientation & Operations Course
JTTF	Joint Terrorism Task Force
LHM	Letterhead Memorandum
MAOP	FBI Manual of Administrative Operations and Procedures
MIOG	FBI Manual of Investigative Operations and Guidelines
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCIS	Naval Criminal Investigation Service
NCTC	National Counterterrorism Center
[redacted]	
NF	Distribution to non-US citizens is prohibited, regardless of their clearance or access permissions
NFIPM	National Foreign Intelligence Program Manual
NFPO	No Foreign Policy Objection
NHCD	National HUMINT Collection Directives
NIPF	National Intelligence Priorities Framework
NISS	National Information Sharing Strategy
NOFORN	Distribution to non-US citizens is prohibited, regardless of their clearance or access permissions
NJTTF	National Joint Terrorism Task Force
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSIG	Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection
NSL	National Security Letter
NSLB	National Security Law Branch
NSPD	National Security Presidential Directive
OC	Originator controls dissemination and/or release of the document
OGC	FBI Office of the General Counsel
OI	Office of Intelligence, DOJ NSD
OIC	FBI Office of Integrity and Compliance
OMB	Office of Management and Budget
OO	Office of Origin
ORCON	Originator controls dissemination and/or release of the document
PCLU	FBI Privacy and Civil Liberties Unit
PI	Preliminary Investigation
PG	Policy Implementation Guide
PIOB	FBI Potential Intelligence Oversight Board
P.L.	Public Law
RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
S	Secret

SA	Special Agent
SAC	Special Agent in Charge
SAN	Storage Area Network
SCI	Sensitive Compartmentalized Information
SCION	Sensitive Compartmentalized Information Operational Network
SMP	Standard Minimization Procedure
SMS	Short Message Service (text messages)
SOG	FBI Special Operations Group
SORC	FBI Sensitive Operations Review Committee
SSA	Supervisory Special Agent
STAO	FBI Special Technologies & Applications Office
STAS	FBI Special Technologies & Applications Section
SWT	*Subhanahu wa ta'ala* (Arabic phrase meaning "Glory to God")
TCP/IP	Transmission Control Protocol/Internet Protocol
TICTU	FBI Telecommunications Intercept and Collection Technology Unit
TFO	Task Force Officer
TREC	Text Retrieval Conference
TS	Top Secret
TT	Trap and Trace
UC	Undercover
UCE	Undercover Employee
UCFN	FBI Universal Case File Number
UCRC	FBI Undercover Review Committee
UDP	Undisclosed Participation
UNI	FBI Universal Index
USAO	United States Attorney's Office
U.S.C.	United States Code
USIC	United States Intelligence Community
USMS	United States Marshals Service
USPER	US Person
VoIP	Voice Over Internet Protocol
WiFi	Limited range wireless communications network
WFO	Washington, D.C., Field Office
WRAMC	Walter Reed Army Medical Center

EXHIBIT 1

Letter dated August 6, 2010,

from

Laura W. Murphy, Director,
American Civil Liberties Union Washington Legislative Office
and
Anthony D. Romero, Executive Director,
American Civil Liberties Union

to

The Honorable William H. Webster

WASHINGTON
LEGISLATIVE OFFICE

August 6, 2010

The Honorable William H. Webster
Milbank, Tweed, Hadley & McCloy LLP
1850 K Street, NW
Suite 1100
Washington, DC 20006

Dear Judge Webster:

On behalf of the American Civil Liberties Union (ACLU), we write to express our views on current domestic surveillance authorities for your consideration during your review of the incident at Fort Hood, Texas. This memorializes and expands upon conversations between our respective staffs. While we appreciate having the opportunity to engage in those conversations to express our strong concerns with existing surveillance authorities, we have had similar conversations with others in positions of authority over the last several years. We are particularly concerned that those authorities in most cases failed to address our concerns, while at the same time they also attempted to gain favorable treatment in some public spheres by claiming to have 'consulted' civil liberties groups. The Fort Hood killings were a tragic occurrence. But that tragedy must not be compounded by further eroding the privacy, due process, and speech rights of millions of wholly innocent Americans who are absolutely entitled to the full panoply of individual rights enumerated in our Constitution.

In our view, the expansions in the government's surveillance authorities over the last nine years already infringe on civil liberties and should not be amended to grant the government even more expansive powers. Over the past nine years, the government's domestic surveillance powers have changed dramatically. Suspicionless or mass surveillance has replaced the traditional model of surveillance narrowly targeted at those suspected of wrongdoing. Judicial oversight and discretion has been minimized. Since the attacks of September 11, the executive branch has asserted (or obtained from Congress) the authority for the dragnet collection and analysis of innocent Americans' telephone calls and e-mails, web browsing records, financial records, credit reports, and library records. Increasingly, the government is engaged in suspicionless data collection and surveillance that vacuums up and tracks sensitive information about innocent people. Even more disturbingly, as the government's surveillance powers have grown more intrusive and more powerful, the restrictions on many of those powers have been weakened or eliminated. And this surveillance often takes place in secret, with little or no oversight by the courts, by legislatures, or by the public. Instead of further reducing privacy protections in these laws, the government should amend them to require a nexus to suspected terrorist activity. This summary will examine constitutionally-suspect

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202 544 1681
F/202 546 0738
WWW ACLU ORG

LAURA W MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
T/212 549 2500

powers and authorities in several laws and initiatives adopted in the post-9/11 years, including the USA PATRIOT Act, the Foreign Intelligence Surveillance Act Amendments Act of 2008, the Attorney General Guidelines, the FBI Domestic Investigations Operations Guide, Fusion Centers, Suspicious Activity Reporting, and the increased use of Administrative Subpoenas.

The USA PATRIOT Act

On October 26, 2001, former President Bush signed the Patriot Act into law. The Patriot Act vastly – and unconstitutionally – expanded the government's authority to pry into people's private lives with little or no evidence they were doing anything wrong. The expanded Patriot Act surveillance authorities unnecessarily and improperly infringe on Americans' privacy, free speech, and associational rights. Worse, the Patriot Act authorizes the government to engage in increased domestic spying in secret with few, if any, protections built in to ensure these powers are not abused, and little opportunity for Congress to review whether the authorities it granted the executive branch actually made Americans any safer. We are concerned with many Patriot Act authorities, but will focus here on national security letters (NSLs) and three provisions due to expire on February 28, 2011. Our full report on the Patriot Act can be found at www.reformthepatriotact.org.

National security letters are secret letters through which the FBI can demand personal records about innocent customers from ISPs, financial institutions and credit companies without prior judicial approval or any requirement of suspicion. Through NSLs the FBI can demand sensitive information such as financial records, credit reports, telephone and e-mail communications records, and Internet-search activity. The NSL statutes also allow the FBI to impose non-disclosure or "gag orders" that prohibit NSL recipients from disclosing anything about the record demand.

The FBI's NSL authority derives from separate statutes that were significantly expanded by **section 505** of the Patriot Act.[1] **Section 505** increased the number of officials who could authorize NSLs and reduced the standard necessary to obtain information with them. Before enactment of the Patriot Act, NSLs could be used only to obtain records about people suspected of wrongdoing. Now, the FBI can obtain sensitive customer records merely by certifying to itself that the records sought are "relevant" to an authorized counterterrorism or counter-intelligence investigation. Thus, the NSL statutes now allow the FBI (and some other executive branch agencies) to obtain records about people who are not known – or even suspected – to have done anything wrong. The Patriot Act reauthorization made the NSL provisions permanent.

The Department of Justice Inspector General ("IG") has conducted a number of audits of the FBI's use of the intrusive NSL record demand power. Each of these audits revealed FBI abuse and mismanagement of the NSL authority. The first two IG audits,

[1] The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).

covering NSLs and section 215 orders the FBI issued from 2003 through 2005, were released in March of 2007.[2] They confirmed widespread FBI mismanagement, misuse and abuse of these Patriot Act authorities, just as the ACLU had warned.[3] The NSL audit revealed that the FBI so negligently managed its use of NSLs that it literally did not know how many NSLs it had issued. As a result, the FBI had seriously under-reported its use of NSLs in previous reports to Congress. The IG also found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes and often used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the files the IG audited contained unreported legal violations.[4] Finally, and most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[5]

On March 13, 2008, the IG released a second pair of audit reports which covered 2006 and evaluated the reforms implemented by the DOJ and the FBI after the first audits were released in 2007.[6] Not surprisingly, the new reports identified many of the same problems discovered in the earlier audits. The 2008 NSL report showed that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirmed the FBI was increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[7] The 2008 IG audit also revealed that high-ranking FBI officials, including an assistant director, a deputy assistant director, two acting deputy directors and a special agent in charge, improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[8] The IG reported that none of these "blanket NSLs" complied with FBI policy and eight imposed non-disclosure requirements on recipients that did not comply with the law.[9] Moreover, it is clear from the IG report that the NSLs were written to "cover information already acquired through exigent letters and other informal responses."[10] The IG expressed concern that such high-ranking officials would fail to comply with FBI policies requiring FBI lawyers to review all NSLs, but it seems clear enough that this step was intentionally avoided because the officials knew

---

[2] See below for discussion of Section 215 orders.

[3] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter 2007 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter 2007 Section 215 Report].

[4] 2007 NSL Report, *supra* note 3, at 84.

[5] 2007 NSL Report, *supra* note 3, at 86-99.

[6] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf [hereinafter 2008 Section 215 Report].

[7] 2008 NSL Report, *supra* note 6, at 9.

[8] 2008 NSL Report, *supra* note 6, at 127, 129 n.116.

[9] 2008 NSL Report, *supra* note 6, at 127.

[10] 2008 NSL Report, *supra* note 6, at 127.

these NSL requests were illegal.[11] It would be difficult to call this conduct anything but intentional. In the face of such abuses, and in consideration of the ever expanding collection of sensitive records, the NSL statutes should be amended to limit the FBI's authority to issue NSLs only where the person whose records are sought is a suspected terrorist, and to issue exigent letters only when harm is imminent and compliance with the NSL process would cause undue delay.

National security letter gag orders. The ACLU challenged the constitutionality of NSL gag orders in three cases. In one of these cases, *Doe v. Holder*, the ACLU twice has successfully challenged the constitutionality of the non-disclosure provisions of the NSL statue itself. In 2004, a district court judge ruled that the NSL statute's automatic gag provisions violated the First Amendment. In response to that ruling, Congress amended the NSL statute, remedying some problems but worsening others. In particular, the NSL statute's gag provisions remained unconstitutional and the ACLU continued to challenge the amended provisions in Court. In December 2008, the U.S. Court of Appeals for the Second Circuit ruled that parts of the revised NSL statute's gag provisions were unconstitutional. Specifically, the court ruled unconstitutional the sections that wrongly placed the burden on NSL recipients to challenge gag orders, that narrowly limited judicial review of gag orders, and that required courts to defer entirely to the executive branch. Congress must amend the non-disclosure statute to require the government to demonstrate that national security would be harmed in the absence of the gag and ensure that the gag automatically expires when that threat no longer exists.

Section 206 of the Patriot Act authorizes the government to obtain "John Doe roving wiretap" orders from the Foreign Intelligence Surveillance Court (FISC) that do not identify either the communications device to be tapped nor the individual against whom the surveillance is directed.[12] While the provision requires the target to be described "with particularity," and the FBI to file an after-the-fact report to the FISC to explain why the government believed the target was using the phones it was tapping, it vests government agents with an inappropriate level of discretion reminiscent of the general warrants that so angered American colonists prior to our country's founding. There is little public information available regarding how the government uses section 206. It should be amended to reflect the criminal standard to require the order to identify either the device or individual being tapped.

Section 6001 of the Intelligence Reform and Terrorism Prevention Act, which is known as the "lone wolf" provision, authorizes the government to obtain secret FISA surveillance orders against non-U.S. persons[13] who are not even believed to be connected to any international terrorist group or foreign nation.[14] The government justified this provision by imagining a hypothetical "lone wolf," an international terrorist operating independently of any terrorist organization, but there is little evidence to suggest this imaginary possibility was a real problem. As of the fall of 2009, this authority has never

[11] 2008 NSL Report, *supra* note 6, at 130.
[12] 50 U.S.C. §§ 1804-05.
[13] 50 U.S.C. § 1801(i).
[14] 50 U.S.C. § 1801(b)(1)(C).

been used.[15] However, since terrorism is a crime, there is no reason to believe that the government could not obtain a Title III surveillance order from a criminal court if the government had probable cause to believe such an individual was planning an act of terrorism. Quite simply, this provision allows the government to avoid the more exacting standards and heightened accountability associated with obtaining electronic surveillance orders from criminal courts. The lone wolf authority should be repealed.

Section 215 of the Patriot Act is a sweeping grant of authority that gives the government the power to obtain secret FISC orders demanding "any tangible thing" from anyone and about anyone it claims is relevant to an authorized investigation regarding international terrorism or espionage. Known as the "library records provision," section 215 significantly expands the types of items the government can demand and obtain under FISA, and lowers the standard of proof necessary to obtain an order from the FISC. Until the enactment of the Patriot Act, the government was required to show probable cause to believe the target of a demand was an agent of a foreign power. Section 215 of the Patriot Act lowered that standard significantly. Now the government only needs to state that the items sought are relevant to an authorized investigation. Indeed, the FBI no longer even needs to show that the items sought pertain to a person the FBI is investigating. Thus, under section 215, the government can obtain orders to obtain private records or items belonging to people – including U.S. citizens and residents – who are not even under suspicion of involvement with terrorism or espionage. Although some government officials have complained that the 215 process is already too onerous, an IG investigation found that the delays in obtaining information were the result of unfamiliarity with the proper process, simple misrouting of the section 215 requests, and an unnecessarily bureaucratic, self-imposed, multi-layered review process.[16] To prevent the collection of wholly innocent information, this provision should be limited to collection of information on agents of foreign powers.

Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA)

The FISA Amendments Act (FAA) permits the executive branch to engage in dragnet surveillance of Americans' international telephone calls and e-mails without a warrant, without suspicion of any kind, and with only very limited judicial oversight.[17] Its most important limiting factor, that the "targets" of FAA surveillance must be people reasonably believed to be overseas, is of little comfort to the Americans who are on the other end of those communications. Americans do not lose their privacy and free speech rights just because they communicate with people abroad.

The FAA requires only minimal court oversight of this spying authority. In assessing an FAA surveillance application, the FISC reviews only the government's proposed, general procedures for targeting and minimizing the use of information that is

---

[15] *Reauthorizing the USA PATRIOT Act Ensuring Liberty and Security Before the Senate Comm on the Judiciary*, 110th Cong (2009) (statement of David Kris, Assistant Attorney General) *available at* http //judiciary.senate gov/pdf/09-09-23%20Kris%20Testimony.pdf

[16] 2008 Section 215 Report, *supra* note 6, at 45-47.

[17] 50 U S C. § 1881-1881f.

collected. The Act does not require the government to demonstrate to the FISC that its surveillance targets are foreign agents, that they are engaged in criminal activity, or that they are connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed.

Thus, the government may obtain an FAA surveillance order without identifying the people (or even the group of people) to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without specifying the particular communications to be collected; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and without making even a prior administrative determination that the acquisition relates to a particular foreign agent or foreign power. An FAA surveillance order is intended to be a kind of blank check, which once obtained will suffice to cover – without further judicial authorization – whatever surveillance the government may choose to initiate, within broadly drawn parameters, for a period of up to one year. Thus, the court may not know who, what, or where the government will actually tap, thereby undercutting any meaningful role for the court and violating the Fourth Amendment. A single FAA order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

The FAA does contain a general ban on reverse targeting, the practice of continuing a wiretap on a person overseas as a pretext for listening in on a U.S. target. However, it lacks stronger language contained in prior House legislation that required clear statutory directives about when the government should return to the FISA court to obtain an individualized order to continue listening to a U.S. person's communications. The trigger for individualized probable cause warrants is instead negotiated between the administration and the secret FISA court.

The FISA Amendments Act should be repealed. The Fourth Amendment requires issuance of warrants to conduct a wiretap of Americans' communications. The Fourth Amendment also requires those warrants to describe with particularity the persons or places to be tapped. Moreover, surveillance authorities, in order to be deemed reasonable under the Fourth Amendment, must have "precise and discriminate" requirements that "carefully circumscribed" the government's spying power "so as to prevent unauthorized invasions of privacy."[18] While we support amendments that would reduce the collection of innocent U.S. communications and information, such as banning bulk collection programs or strict minimization requirements, any collection under this program is unconstitutional. The ACLU is challenging this law in court.[19]

---

[18] Berger v. New York, 388 U.S. 41, 57-58 (1967)

[19] Amnesty v. Blair Complaints, motions and declarations *available at* http://www.aclu.org/national-security/amnesty-et-al-v-blair.

Attorney General Guidelines

After the revelation of widespread spying on Americans in the 1970s, the Senate convened the Church Committee to investigate government practices and make recommendations about reining them in. Exposure of the FBI's COINTELPRO program, led to a series of reforms, including laws designed to regulate government surveillance and internal guidelines, now referred to as the Attorney General's Guidelines, which limited the FBI's investigative authority and spelled out the rules governing law enforcement operations. The most recent and dramatic changes to the AG Guidelines were made in December 2008, in the Bush Administration's final month in office.[20] Then-Attorney General Michael Mukasey instituted new guidelines that authorize the FBI to conduct investigations, called "assessments", without requiring any factual predicate suggesting the involvement of the target of the investigation in illegal activity or threats to national security. The Supreme Court established "reasonable suspicion" as the standard for police stops in *Terry v Ohio* in 1968. This standard required suspicion supported by articulable facts suggesting criminal activity was afoot before a policeman could stop a person for investigative purposes. Likewise, the Department of Justice established a reasonable suspicion standard for the inclusion of personally identifiable information into criminal intelligence systems. The Mukasey guidelines, however, allow the FBI to utilize a number of intrusive investigative techniques during these assessments, including physical surveillance, retrieving data from commercial databases, recruiting and tasking informants to attend meetings under false pretenses, and engaging in "pretext" interviews in which FBI agents misrepresent their identities in order to elicit information "Assessments" can even be conducted against an individual simply to determine if he or she would be a suitable FBI informant. Nothing in the new AG Guidelines protects entirely innocent Americans from being thoroughly investigated by the FBI for no good reason. The new Guidelines explicitly authorize the surveillance and infiltration of peaceful advocacy groups in advance of demonstrations, and they do not clearly prohibit using race, religion, or national origin as factors in initiating assessments.

Innocence no longer protects ordinary Americans from being subjected to a wide range of intrusive investigative techniques such as collecting information from online sources, including commercial databases, recruiting and tasking informants to gather information, using FBI agents to gather information surreptitiously from someone without revealing their true identity or true purpose for asking questions, and having FBI agents follow them day and night for as long as they want. The new guidelines also open the door to racial profiling. They "do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," but that policy included an exemption for national security and border integrity investigations.[21]

---

[20] DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC OPERATIONS, DEPARTMENT OF JUSTICE, *available at* http //www justice gov/ag/readingroom/guidelines pdf, *see also* ACLU, Fact Sheet -Attorney General Guidelines, Oct 8, 2008, *available at* http //www aclu org/national-security/fact-sheet-new-attorney-general-guidelines

[21] U S DEPARTMENT OF JUSTICE, CIVIL RIGHTS DIVISION, GUIDANCE REGARDING THE USE OF RACE BY FEDERALLAW ENFORCEMENT AGENCIES (June 2003), *available at*

By erasing the line between criminal investigations and national security investigations, the guidelines open the door to racial profiling. The Guidelines should be amended to require a factual predicate before investigations are started, a complete ban on racial profiling, and stronger protections for First Amendment protected activity.

Federal Bureau of Investigation Domestic Investigations Operations Guide (DIOG)

An internal FBI guide to implementing the new AG Guidelines, called the Domestic Investigations and Operations Guide (DIOG),[22] contains startling revelations about how the FBI is using race and ethnicity in conducting assessments and investigations. Instead of further limiting the use of race in investigations, it expounds the many ways that it can be incorporated into suspicionless surveillance and information collection. First, the DIOG says that investigative and intelligence collection activities must not be based "solely on race." But the Department of Justice's 2003 Guidance on the Use of Race in Federal Law Enforcement,[23] which is binding on the FBI, says race can't be used "to any degree" absent a specific subject description. This appears to subvert the more exacting limitation.

Moreover, the DIOG describes the authorized uses of race and ethnicity for FBI agents, which include "collecting and analyzing" racial and ethnic community demographics,[24]and collecting "specific and relevant" racial and ethnic behavior. Though the DIOG prohibits "the collection of cultural and behavioral information about an ethnic community that bears no relationship to a valid investigative or analytical need," it allows FBI agents to consider "focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community," as well as "behavioral and cultural information about ethnic or racial communities" that may be exploited by criminals or terrorists "who hide within those communities."[25] The DIOG grants the FBI far too much authority to target racial, ethnic and religious minorities for unwarranted surveillance. The DIOG should be amended to require a factual predicate before information is collected and a meaningful ban on racial profiling.

Fusion Centers

In November 2007, the ACLU issued its first report on fusion centers, rapidly developing multi-jurisdictional intelligence centers designed to organize local domestic information collection activities into an integrated system that can distribute data both horizontally across a network of fusion centers and vertically, down to local law enforcement and up to the federal intelligence community.[26] With at least 72 around the

---

http://www.justice.gov/crt/split/documents/guidance_on_race.php [hereinafter DOJ Use of Race Guidance].

[22] FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION OPERATIONS GUIDE, *available at* http://www.muslimadvocates.org/DIOGs_Chapter4.pdf [hereinafter DIOG].

[23] DOJ Use of Race Guidance, *supra*, note 21.

[24] DIOG, *supra* note 22, at 32.

[25] DIOG, *supra* note 22, 33-34

[26] ACLU, What's Wrong With Fusion Centers? (Dec. 2007), *available at* http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf..

country, these centers can employ officials from federal, state and local law enforcement and homeland security agencies, as well as other state and local government entities, the federal intelligence community, the military and even private companies, to spy on Americans in virtually complete secrecy. We have recently compiled a website to track known instances of abuse by some of these centers. Information about fusion center spying and the related local, state and federal agencies involved can be found at www.aclu.org/spy-files.

While fusion centers vary widely in what they do, overarching problems with these domestic intelligence operations put Americans' privacy and civil liberties at risk. First, in a multi-jurisdictional environment with ambiguous lines of authority, it is unclear what rules apply and which agency is ultimately responsible for the activities of the fusion center participants. Second, some fusion centers incorporate private sector and military participation, thereby threatening the integrity of current privacy laws and risking the violation of the prohibition on military activity on U.S. soil. Third, federal fusion center guidelines encourage wholesale data collection and data manipulation processes that threaten privacy. And finally, fusion centers are characterized by excessive secrecy which limits public oversight and accountability. Moreover, the over-classification of national security information limits its distribution to and from the fusion centers, impairing their ability to acquire essential information and impeding their ability to fulfill their stated mission of sharing information with all appropriate stakeholders, including the public. Excessive secrecy cripples fusion centers' ability to effectively share information, bringing their ultimate value into doubt.".

A number of troubling fusion center intelligence products have leaked to the public. In one, a Texas fusion center intelligence bulletin described a purported conspiracy between Muslim civil rights organizations, lobbying groups, the anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip hop bands to spread Sharia law in the U.S.[27] In another, a Missouri Fusion Center released a report on "the modern militia movement" that claimed militia members are "usually supporters" of third-party presidential candidates like Ron Paul and Bob Barr.[28] Also, a March 2008 Virginia Fusion Center terrorism threat assessment described the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats. Finally, a Washington fusion center reported on protesters on both sides of the abortion debate, despite the fact that no violence was expected.[29] These bulletins, which are widely distributed, would be laughable except that they come with the imprimatur of a federally backed intelligence operation, and they reflect a status quo that apparently condones and encourages law enforcement officers to monitor the activities of political activists and racial and religious minorities.There is some good news, however.

---

[27] TEXAS FUSION CENTER SYSTEM, PREVENTION AWARENESS BULLETIN (Feb 19, 2009), *available at* http://www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf.

[28] MISSOURI INFORMATION ANALYSIS CENTER, THE MODERN MILITIA MOVEMENT (Feb 20, 2009), *available at* www.infowars.com

[29] Ryan J. Foley, Associated Press, *Homeland Security Collected Information on Wisconsin Abortion, Pro-Life Activist,* AP, Feb 8, 2010.

The 2010 DHS Homeland Security Grant Program established a requirement[30] that fusion centers certify that privacy and civil liberties protections are in place in order to use DHS grant funds. This is the first time DHS has acknowledged its authority to regulate fusion center activities and it coincides with the establishment of a new DHS Joint Fusion Center Program Management Office to oversee DHS support to fusion centers.[31] While these are only small steps, they are important advances toward establishing an effective governance and oversight structure for fusion centers. Many fusion centers have also made efforts to address our concern about excessive secrecy surrounding their activities by engaging with local privacy and civil liberties groups, and arranging tours and/or public meetings within their communities. Several fusion centers have sought feedback from privacy and civil liberties groups as they develop their privacy policies. These are welcome opportunities for members of the public to learn about fusion center activities and for fusion center personnel to hear, understand and address public concerns. Finally, the Naval Postgraduate School Center for Homeland Defense and Security initiated a Fusion Center Leaders Program that may help to train, standardize and professionalize fusion center staff.

Suspicious Activity Reporting

Over the last few years, federal, state and local authorities have initiated "suspicious activity reporting" (SAR) programs to encourage law enforcement officers, intelligence and homeland security officials, emergency responders, and even the public to report the "suspicious" activities of their neighbors to law enforcement and intelligence agencies.[32] Law enforcement agencies have long collected information about their routine interactions with members of the public. Sometimes called "field interrogation reports" or "stop and frisk" records, this documentation, on the one hand, provides a measure of accountability over police activity. But it also creates an opportunity for police to collect the personal data of innocent people and put it into criminal intelligence files with little or no evidence of wrongdoing. As police records increasingly become automated, law enforcement and intelligence agencies are increasingly seeking to mine this routine contact information and distribute it broadly, as if it is criminal intelligence information. These SARs programs have aggressively expanded these efforts in the name of national security.

The problem is that many of the behaviors these SAR programs identify as precursors to terrorism include innocuous and commonplace activities such as using

---

[30] DHS/DOJ FUSION PROCESS TECHNICAL ASSISTANCE PROGRAMS AND SERVICES, FACT SHEET: ENHANCING THE PRIVACY, CIVIL RIGHTS AND CIVIL LIBERTIES FRAMEWORK FOR STATE AND MAJOR URBAN AREA FUSION CENTERS, *available at* http://nsi.ncirc.gov/documents/FS_Enhancing_the_Privacy_for_State_and_Major_Urban_Area_FCs.pdf.

[31] *Office of Intelligence and Analysis' Vision and Goals Hearing Before House Committee on Homeland Security*, 110th Cong. (2010) (statement of Caryn Wagner, Under Secretary and Chief Intelligence Officer, Dep't of Homeland Security, and Bart Johnson, Principal Deputy Under Secretary, Dep't of Homeland Security).

[32] MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS (Nov. 5, 2009).

binoculars, taking pictures, drawing diagrams, and taking notes.[33] SAR programs increase the probability that innocent people will be stopped by police and have their personal information collected for inclusion in law enforcement and intelligence databases. They also open the door to racial profiling and other improper police practices by giving police unwarranted discretion to stop people who are not reasonably suspected of wrongdoing. With new intelligence sharing systems like fusion centers, Joint Terrorism Task Forces, and the Director of National Intelligence (DNI) Information Sharing Environment (ISE), information collected by local police in any city or small town in America can now quickly end up in federal intelligence databases.

In January 2008 the DNI ISE program manager published functional standards for state and local law enforcement officers to report 'suspicious' activities to fusion centers and to the federal intelligence community through the ISE. The ACLU released a report criticizing these programs and in response, ISE program manager Thomas E. McNamara and his office worked with the ACLU and other privacy and civil liberties groups, as well as the LAPD and other federal, state and local law enforcement agencies, to revise the ISE SAR functional standard to address privacy and civil liberties concerns.

The revised ISE guidelines for suspicious activity reporting, issued in May 2009, establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement officers may collect Americans' personal information and share it within the ISE. It affirms that all constitutional standards applicable to ordinary criminal investigations, such as the Terry reasonable suspicion test, also apply to SAR inquiries.[34] The revised ISE functional standards also make clear that behaviors such as photography and eliciting information are protected under the First Amendment, and require additional facts and circumstances giving reason to believe the behavior is related to crime or terrorism before reporting is appropriate.[35] These changes to the standard, which include reiterating that race, ethnicity and religion cannot be used as factors that create suspicion,[36] give law enforcement all the authority it needs while showing greater respect for individuals' privacy and civil liberties. We applaud the willingness of the ISE Program Manager to engage constructively with the civil liberties community and to make significant modifications to the functional standard to address the concerns presented. However, ISE is one of only many SAR collection programs across the country. It is critical that operations at the state and local level and those conducted by other federal agencies adopt similar policies to reduce inappropriate law enforcement contact with completely innocent Americans.

---

[33] Mike German and Jay Stanley, ACLU, Fusion Center Update (July 2008), *available at* http://www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf .

[34] INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) VERSION 1.5, at 7, *available at* http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf [hereinafter ISE Standards].

[35] ISE Standards, *supra* note 34 at 29.

[36] ISE Standards, *supra* note 34 at 7, 29.

Possible Expansions of Government Authority: Administrative Subpoenas

Your staff asked us to share our opinion on the expansion of the current national security letter authority to create a general administrative subpoena for national security purposes. As discussed above, we believe that the government is already abusing its NSL authority to collect data on those who are not suspected of any wrongdoing. Expanding the NSL authority to compel the production of any tangible thing or any type of record will only exponentially increase the amount of innocent and irrelevant information in the government's hands and violate the privacy of countless additional people.

Compulsory government demands for information have a number of limiting factors: who issues the demand, the scope of the information obtained, and on what showing the government must make to obtain it. An administrative subpoena would incorporate the lowest possible standard in all of these categories to create a powerful tool that is void of prior judicial authorization, is limitless in its application, and as proposed by a number of sources, would permit collection information on wholly innocent people as long as it is deemed "relevant."

The government has other tools at its disposal and does not need to expand its administrative subpoena capacity. It can obtain a subpoena in a criminal terrorism investigation or apply to the FISC for an order for any tangible thing. It can also use FAA programmatic orders to collect information if those programs are targeted at people believed to be overseas. No one has claimed that these tools are ineffective in obtaining information – only that the required processes are administratively burdensome. Those processes, however, are the only checks on incredibly powerful surveillance authorities that operate in almost complete secrecy and have been shown to be subject to abuse. We should not be looking to expand the opportunity for abuse, but rather to instill discipline and integrity into the process while allowing investigators to do their work in a constitutional manner.

Some also argue that because a small handful of agencies and U.S. Attorneys have criminal subpoena power,[37] the FBI or the intelligence community should have the intelligence equivalent. That others have this power is not germane to the debate of whether our government should create another powerful, intrusive tool to obtain sensitive and personal information. On the other hand, it is germane to consider whether any such authority respects the constitutional rights of those it impacts.

Nearly all agency subpoenas are used for traditional administrative purposes, and only a few are intended to be used as criminal investigative tools.[38] These are designed for very narrow special needs cases, yet a foreign intelligence subpoena would be expansive, purposely including information wholly unrelated to suspected wrongdoing.

---

[37] *See* CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, ADMINISTRATIVE SUBPOENAS AND NATIONAL
SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS, April 15, 2005 (review of federal administrative subpoenas).

[38] *Id.* at 13-18.

Foreign intelligence investigations are fundamentally different from other traditional administrative proceedings in that they are cloaked in secrecy and the information obtained in them is retained, data mined, disseminated or made accessible to countless federal, state and local law enforcement and intelligence staff, and used in undisclosed ways. A new subpoena power would be wholly different from its criminal or administrative counterpart as it would lack many of the limitations and protections that the latter offer.[39] Grand jury subpoenas are also significantly different from recent subpoena power proposals[40] The grand jury is an ancient authority and its independence from the prosecution is well settled. Grand jurors are ordinary citizens tasked with finding probable cause of a crime and to operate as a check on the executive branch, and federal prosecutors are bound by a professional code of ethics. None of these protections would be present in an intelligence subpoena.

Conclusion

We appreciate your soliciting our thoughts on current national security surveillance authorities. The government has expansive powers that are routinely abused to collect information on innocent people in violation of their civil liberties. We hope that your review will conclude that these authorities need to be curtailed to comport with the Constitution and should in no way be expanded. We remain available to discuss in more detail these and any other authorities you are reviewing.

Sincerely,

Laura W. Murphy
Director, ACLU Washington Legislative Office

Anthony D. Romero
Executive Director, ACLU

Cc: Director Robert S. Mueller, Federal Bureau of Investigation
General Counsel Valerie Caproni, Federal Bureau of Investigation
Mr. Adrian Steel, Mayer Brown

[39] For a more complete discussion on a previous subpoena proposal, *see* ACLU, Why FBI Intelligence Subpoenas Threaten Civil Liberties, June 28, 2005, *available at* http //www aclu org/national-security/why-fbi-intelligence-subpoenas-threaten-civil-liberties

[40] *Id*, Coalition Letter to the Select Senate Intelligence Committee, opposing national security subpoenas, May 23, 2005, *available at* http //www aclu org/national-security/coalition-letter-senators-roberts-and-rockefeller-opposing-administrative-subpoena