The Federal Bureau of Investigation and Terrorism Investigations

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism

December 28, 2011

Congressional Research Service
7-5700
www.crs.gov
R41780

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The Federal Bureau of Investigation (FBI, the Bureau) is the lead federal law enforcement agency charged with counterterrorism investigations. Since the September 11, 2001 (9/11) attacks, the FBI has implemented a series of reforms intended to transform itself from a largely reactive law enforcement agency focused on investigations of criminal activity into a more proactive, agile, flexible, and intelligence-driven agency that can prevent acts of terrorism.

This report provides background information on key elements of the FBI terrorism investigative process based on publicly available information. It discusses

- several enhanced investigative tools, authorities, and capabilities provided to the FBI through post-9/11 legislation, such as the USA PATRIOT Act of 2001; the 2008 revision to the *Attorney General's Guidelines for Domestic FBI Operations* (Mukasey Guidelines); and the expansion of Joint Terrorism Task Forces (JTTF) throughout the country;
- intelligence reform within the FBI and concerns about the progress of those reform initiatives;
- the FBI's proactive, intelligence-driven posture in its terrorism investigations using preventative policing techniques such as the "Al Capone" approach and the use of agent provocateurs; and
- the implications for privacy and civil liberties inherent in the use of preventative policing techniques to combat terrorism.

This report sets forth possible considerations for Congress as it executes its oversight role. These issues include the extent to which intelligence has been integrated into FBI operations to support its counterterrorism mission and the progress the Bureau has made on its intelligence reform initiatives.

Contents

Figures

Contacts

Introduction

The Federal Bureau of Investigation (FBI, the Bureau) is the lead agency for investigating the federal crime of terrorism,[1] which is defined under law as "an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct."[2] This includes terrorist acts committed within and outside U.S. national boundaries.[3] This report provides background on some of the key elements of the FBI terrorism investigative process based on publicly available information.

The September 11, 2001 (9/11) terrorist attacks have been called a major security, law enforcement, and intelligence failure.[4] Prior to 9/11, the FBI was largely a reactive law enforcement agency—pursuing suspects after they had allegedly committed crimes. Since 9/11, the Bureau has arguably taken a much more proactive posture, particularly regarding counterterrorism.[5] It now views its role as both "predicting and preventing" the threats facing the nation, drawing upon enhanced resources.[6] A few basic measures suggest this:

- Post-9/11 legislation—notably the USA PATRIOT Act (P.L. 107-56)—dismantled "the Wall" between intelligence and criminal investigation and expanded the U.S. government's ability to monitor terrorist suspects, among other changes.
- Changes in the *Attorney General's Guidelines for Domestic FBI Operations* and the *FBI Domestic Investigations and Operations Guidelines* give the FBI more leeway to engage in proactive investigative work that does not depend on criminal predication (i.e., a nexus to past or future criminal activity).
- Since 9/11, a widening of the agency's counterterrorism operations has occurred as well as closer liaison with agencies outside the Department of Justice (DOJ). This is most evident domestically in the increased number of its Joint Terrorism

[1] Pursuant to 28 C.F.R. 0.85(l), the Attorney General has assigned responsibility to the Director of the FBI to "(l) Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate." If another federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI.

[2] 18 U.S.C. 2332b(g)(5)(A). Subparagraph B enumerates the specific crimes covered by this definition. The FBI differentiates hate crimes and other criminal activity from domestic terrorism partly by assessing the intent of the criminals involved in specific incidents. Hate crimes "generally involve acts of personal malice directed at individuals" and lack the broader motivations and driving acts of domestic terrorism. In addition, the lines are not always clear between ordinary criminal acts and domestic terrorism. In these instances, FBI investigations also focus on clarifying the motives of the suspects involved—such as profit, personal malice, or an ideologically driven agenda.

[3] The extraterritorial jurisdiction for terrorism crimes is specified in 18 U.S.C. 2332b(e) and (f).

[4] The National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, p. xvi. The Commission specifically attributed the 9/11 attacks to failures in four areas: imagination, policy, capabilities, and management. See p. 339.

[5] The FBI describes the post-9/11 changes in its approach in all major program areas at "The Intel-Driven FBI: New Approaches," http://www.fbi.gov/about-us/intelligence/intel-driven/new-approaches.

[6] U.S. Congress, House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, *Statement of Robert S. Mueller, III; Director FBI*, Federal Bureau of Investigations FY2012 Budget Hearing, 112th Cong., 1st sess., April 6, 2011, http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012. (Hereafter: Mueller Testimony, April 6, 2011.)

Task Forces (JTTF). These are multi-agency investigative units led by DOJ and the FBI and are designed to combine the resources of federal, state, and local law enforcement. They are locally based and comprised of investigators, analysts, linguists, Special Weapons and Tactics (SWAT) experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies.[7] In 1999, there were 26 JTTFs throughout the United States.[8] As of December 2011, there were over 100.

- Evidence of growth within the FBI's counterterrorism operations can also be seen in the agency's increased allocation of agents to terrorism matters. In April 2011 testimony to Congress, FBI Director Robert Mueller "estimated that before 9/11, there were 10,000 FBI agents on the streets, with 30 percent engaged in national security issues and the rest focused on criminal activity. Since then, Mueller said, he has gained 4,000 more agents and the FBI's focus is a 50-50 split between terrorism and other criminal activity like mortgage fraud."[9]
- To further its proactive intelligence-driven counterterrorism mission, the FBI established a National Security Branch (NSB) and a Directorate of Intelligence (DI) within the NSB. Moreover, the FBI has reportedly increased its intelligence analyst workforce from approximately 1,100 in October 2001 to more than 3,000 by September 2011.[10]

Enhanced Investigative Authorities, Tools, and Capabilities

The FBI is an intelligence agency as well as a law enforcement agency.[11] Since 9/11, the Bureau has taken what it describes as a more forward-leaning, intelligence-driven posture in its terrorism investigations in order to prevent or disrupt terrorist acts, not merely investigate them after they have occurred. Shortly after the attacks, FBI Director Robert Mueller wrote a memo to Special Agents in Charge of FBI Field Offices saying, "while every office will have different crime problems that will require varying levels of resources, the FBI has just one set of priorities: *Stop the next attack*."[12] Then-Deputy Attorney General Paul McNulty described the DOJ's aggressive, proactive, and preventative approach as

[7] DOJ, *Joint Terrorism Task Force,* http://www.justice.gov/jttf/.

[8] Federal Bureau of Investigation (FBI), *Terrorism in the United States: 1999,* p. 44.

[9] Phillip Swarts, "Director Warns Shutdown Would Harm FBI," upi.com, April 7, 2011, http://www.upi.com/Top_News/Special/2011/04/07/Director-warns-shutdown-would-harm-FBI/UPI-46091302214622/#ixzz1Ix7YBLZ2

[10] Robert S. Mueller, III, Director, Federal Bureau of Investigation, "Statement Before the Senate Committee on Homeland Security and Governmental Affairs" September 13, 2011, http://www.fbi.gov/news/testimony/ten-years-after-9-11-are-we-safer. See also FBI Intelligence Analysts Association, "About FBI Intelligence Analysts," http://www.fbianalysts.org/about.aspx; and Mueller Testimony, April 6, 2011.

[11] FBI, *Domestic Investigations and Operations Guide,* (DIOG) redacted, December 16, 2008, p. 3, available at http://www.eff.org/fn/directory/8364/354. (Hereafter: DIOG, redacted.)

[12] Garrett M. Graff, *The Threat Matrix: The FBI at War in the Age of Terrorism* (New York: Little Brown and Co., 2011), p. 404. (Hereafter: Graff, *The Threat Matrix.*) Chapter 11 of the book discusses the pressure brought to bear on the FBI immediately after 9/11 to prevent future attacks. The author also reports that some former and current FBI special agents who worked in counterterrorism dispute the notion that prevention of terrorism only became a priority after 9/11. See pp. 426-430.

> the only acceptable response from a department of government charged with enforcing our laws and protecting the American people. Awaiting an attack is not an option. That is why the Department of Justice is doing everything in its power to identify risks to our Nation's security at the earliest stage possible and to respond with forward-leaning – preventative – prosecutions.[13]

The FBI's post-9/11 transformation is particularly evident in four areas: The USA PATRIOT Act provided the FBI additional authorities and enhanced investigative tools.[14] The FBI and DOJ altered the way the agency investigated terrorism with the 2008 revision of *The Attorney General's Guidelines for Domestic FBI Operations*. The FBI expanded operationally via a proliferation of JTTFs across the United States. In so doing, it also increased its cooperation with state, local, and federal agencies. Finally, watershed changes were made in the Bureau's intelligence program.

USA PATRIOT Act

Shortly after the 9/11 attacks, Congress provided the FBI with several additional investigative tools and expanded its authority to monitor and search suspects in terrorism-related and other investigations. Many of these tools and authorities were contained in the USA PATRIOT Act (P.L. 107-56) signed by President George W. Bush on October 26, 2001. The act amended several existing statutes, such as the Foreign Intelligence Surveillance Act (FISA) of 1978 (P.L. 95-511), the Electronic Communications Privacy Act of 1986 (P.L. 99-508), and the various National Security Letter (NSL) statutes.[15] Additional tools and authorities include

- dismantling "the Wall" that inhibited the sharing of information between intelligence and criminal investigators,
- roving wiretaps,
- expanded use of devices that record the sources of incoming and outgoing communications,
- "Sneak and Peek" search warrants,
- increased access to business records, and
- expanded use of National Security Letters.

Dismantling "the Wall" Between Intelligence and Criminal Investigations

Historically, there have been differences between electronic surveillance (wiretaps) conducted for intelligence and for law enforcement purposes. Among these is the protection of the constitutional rights of persons under criminal investigation. A former government official describes the differences:

---

[13] Prepared Remarks of Deputy Attorney General Paul J. McNulty at the American Enterprise Institute, Washington, D.C., May 24, 2006, http://www.justice.gov/archive/dag/speeches/2006/dag_speech_060524.html.

[14] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107-56.

[15] For more information on these authorities, see CRS Report R40980, *Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization*, by Edward C. Liu.

> Law enforcement wiretaps are heavily regulated … they can only be carried out for a limited time. They require constant supervision and review…. They are approved for only specific types of crime…. And once a crime begins the defendant can see transcripts of the wiretaps and challenge their legality…. Intelligence wiretaps are different … they aren't triggered by suspected criminal activity. Any representative of a foreign government is fair game for an intelligence tap. The rules that apply to law enforcement taps just aren't appropriate for intelligence wiretaps.[16]

FISA regulates intelligence collection directed at foreign powers and agents of foreign powers in the United States to include those engaged in international terrorism.[17] FISA required the government to certify that "the purpose" of surveillance was to gather foreign intelligence information.[18] Prior to the USA PATRIOT Act, DOJ turned the "primary purpose" standard into written policy that had the effect of limiting the coordination between intelligence and criminal investigators.[19] This came to be known as "the Wall" between intelligence and law enforcement and the "unfortunate consequences" of this barrier to information sharing were noted by the 9/11 Commission in its report on the 9/11 attacks.[20]

Section 218 of the USA PATRIOT Act amended FISA to replace the phrase "the purpose" with the phrase "a significant purpose." According to Senator Dianne Feinstein, these changes were necessary to make it

> easier to collect foreign intelligence information under … FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence. But in today's world things are not so simple. In many cases, surveillance will have two key goals—the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.[21]

As one legal scholar described it, by moving the FISA requirement from *the* purpose to *a significant purpose*, the USA PATRIOT Act "knocked out the foundation for 'the Wall.'"[22] This removed impediments to the exchange of information about terrorism or other national security threats between intelligence and law enforcement personnel.

Other provisions of the USA PATRIOT Act also sought to increase intelligence information sharing. Section 504 amended FISA by adding provisions allowing federal officers who conduct electronic surveillance to acquire foreign intelligence information to consult with federal law

---

[16] Stewart Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* (Stanford, CA: Hoover Institution Press, 2010), pp. 40-1. For further discussion of this issue, see chapter 3. (Hereafter: Baker, *Skating on Stilts.*)

[17] For the definitions within FISA for foreign power and agents of a foreign power, see P.L. 95-511, §101.

[18] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, (Washington, DC: U.S. Government Printing Office, 2004), p.78. (Hereafter: *9/11 Commission Report.*)

[19] Cedric Logan, "The FISA Wall and Federal Investigations," *New York University Journal of Law and Liberty*, vol. 4, no. 209, p. 229. http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_law_and_liberty/documents/documents/ecm_pro_062708.pdf. (Hereafter: Logan, "The FISA Wall and Federal Investigations.")

[20] *9/11 Commission Report,* p. 79 and Chapter 8.

[21] Statement of Senator Dianne Feinstein, 147 Cong Rec. S10591, October 11, 2001, quoted in Logan, "The FISA Wall and Federal Investigations," pp. 230-1. Full statement available at http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi.

[22] Logan, "The FISA Wall and Federal Investigations," p. 230.

enforcement officers to coordinate efforts to investigate or protect against (among other issues) sabotage or international terrorism by a foreign power or an agent of a foreign power.[23] And Section 203 amended the Federal Rules of Criminal Procedure to allow disclosure of grand jury information in certain circumstances, including if that information is related to sabotage or international terrorism by a foreign power or an agent of a foreign power.[24]

Roving Wiretaps

Federal law enforcement officers have the authority, subject to court approval, to conduct wiretaps and electronic surveillance on persons suspected of committing federal crimes. A "roving" wiretap allows law enforcement officers to "follow" a subject and lawfully intercept that person's communications with a single court order even if the target attempts to evade surveillance by changing telephones or other communications devices.[25] According to an Assistant U.S. Attorney, "Prior to roving wiretaps, law enforcement agents and federal prosecutors had to invest substantial time and resources in obtaining a separate wiretap order for each additional telephone used by a subject during an investigation … [Q]uite often this resulted in a loss of valuable evidence through missed wiretap conversations relating to the criminal activity being monitored."[26]

Before the USA PATRIOT Act, the concept behind roving wiretaps did not apply to FISA.[27] The USA PATRIOT Act amended the electronic surveillance portion of FISA to allow government agents to continue surveillance when "the target of the surveillance switches from a facility (e.g., a telephone) associated with one service provider (e.g., a telephone company) to a different facility associated with a different provider."[28]

Expanded Use of Devices that Record the Sources of Incoming and Outgoing Communications

A trap and trace device shows all incoming phone numbers to a particular telephone.[29] A pen register shows all outgoing phone numbers a particular telephone has called.[30] Prior to 2001, FISA allowed law enforcement officers to collect incoming and outgoing numbers on a telephone

[23] P.L. 107-56, §504, (a)(k)(1)(B).

[24] P.L. 107-56, §203, (a)(1)(C)(V).

[25] Peter M. Thomson, "White Paper on The USA PATRIOT Act's 'Roving' Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act," The Federalist Society for Law and Public Policy Studies, April 2004, p. 1, http://www.fed-soc.org/doclib/20070326_rovingsur.pdf.

[26] Ibid.

[27] Ibid, p. 2.

[28] P.L. 107-56, §206. See also U.S. Congress, House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, *USA Patriot Act Reauthorization*, Statement of Todd M. Hinnen, Acting Assistant Attorney General, 112th Cong., 1st sess., March 9, 2011, p. 1.

[29] 18 U.S.C. §3127(3) defines a "trap and trace device" as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

[30] 18 U.S.C. §3127(3) defines a "pen register" as "a device or process which records or decodes routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."

line. The USA PATRIOT Act expanded the law to permit the capture of comparable information related to other forms of communication including the Internet, electronic mail, web surfing, and all other forms of electronic communications.[31]

"Sneak and Peek" Search Warrants

In general, police officers serving a warrant must "knock and announce"—that is, give the subject notice that they are the police and are serving a warrant. They may enter and search even if the subject is not present at the premises to be searched, but they must leave a copy of the warrant and an inventory of what was seized, giving notice that the premises was searched.[32]

The USA PATRIOT Act amended Title 18[33] to allow federal law enforcement officers to request from the courts a delayed-notice (so-called "sneak and peek") search warrant allowing officers to enter and search a premises without immediately notifying the owner when such notice may have an adverse result (e.g., tipping off a suspect or co-conspirators).[34]

This authority has been used rarely in terrorism cases. In the three years for which data are available (October 1, 2006-September 30, 2009), the Director of the Administrative Office of the United States Courts reported to Congress that 2,332 delayed-notice search warrant requests were made. Drug-related offenses accounted for 1,618 (69.4 %) of these. The next largest category of offense for such warrants was fraud (122 warrants, 5.2%). Fifteen requests (less than 1%) were made for terrorism cases.[35]

Increased Access to Business Records

The USA PATRIOT Act amended FISA to authorize the FBI to seek an order from the FISA Court for the production of any tangible things (including books, records, papers, documents, and other items) in a terrorism or counterintelligence investigation provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment.[36]

National Security Letters

National Security Letters (NSL)[37] are regularly used in FBI counterterrorism investigations and are roughly comparable to administrative subpoenas.[38] They have been described as "form letters

[31] P.L. 107-56, §214 and §216.

[32] Electronic Freedom Foundation, "'Sneak and Peek' Search Warrants," https://ssd.eff.org/your-computer/govt/sneak-and-peek.

[33] 18 U.S.C. 3103(a), which amended Rule 41(f)(3) of the Federal Rules of Criminal Procedure.

[34] P.L. 107-56, §213.

[35] Director of the Administrative Office (AO) of the United States Courts, *Report on Applications for Delayed-Notice Search Warrants and Extensions,* for FY2007, FY2008, and FY2009, Table 2. The USA PATRIOT Act requires the AO to transmit to Congress annually (beginning with data from FY2007) a full and complete report summarizing information reported by judges on delayed-notice search warrants.

[36] P.L. 107-56, §215.

[37] For additional information, see CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle.

signed by an FBI agent"[39] used to request and collect non-content consumer records and related information from "telephone companies, Internet service providers, consumer credit reporting agencies, banks, and other financial institutions."[40] The FBI has said that "NSLs are indispensable investigative tools that serve as building blocks in many counterterrorism and counterintelligence investigations."[41] In 2010, the FBI made 24,287 NSL requests. These requests asked for information related to 14,212 different individuals.[42]

NSLs predate the USA PATRIOT Act, but the act increased their use by the FBI.[43] For one thing, the USA PATRIOT Act allowed the FBI to issue NSLs for full consumer credit reports.[44] Additionally, it widened the number of FBI officials who could issue NSLs.[45] It also expanded the circumstances under which the letters could be issued by eliminating requirements that NSLs contain specific and articulable facts demonstrating a nexus to a foreign power or its agents.

(...continued)

[38] CRS Report R41619, *National Security Letters: Proposals in the 112th Congress*, by Charles Doyle, p. 1. (Hereafter: CRS Report R41619.)

[39] Government Relations Office and Government Relations Committee, American Association of Law Libraries (AALL), *National Security Letters,* AALL Issue Brief 2007-2, Revised March 2007, September 2009, December 2009, February 2010, p. 1, http://www.aallnet.org/aallwash/ib032007b.pdf. (Hereafter: AALL, *National Security.*)

[40] CRS Report R41619, p. 1. "Non–content" as it relates to telephone records, does not include the *content* of conversations. Rather, the FBI can request items such as customer identity, length of service, and toll records.

[41] Office of the Inspector General, Department of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters,* March 2007, p. 121, http://www.justice.gov/oig/special/s0703b/final.pdf. Hereafter: DOJ OIG, *Review of FBI Use of NSLs,* March 2007. According to a media report, the FBI's use of business record requests under section 215 of the USA PATRIOT Act increased in 2010—in 2009 the Bureau made 21 requests, and in 2010, it made 96. This increase was reportedly attributable to some communications service providers not providing all information broadly asked for under NSLs. Most business record requests in the first three months of 2011 reputedly involved Internet records. See Ellen Nakashima, "FBI Going to Court More Often to Get Personal Internet-Usage Data," *Washington Post,* October 25, 2011, http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html.

[42] Letter transmitting report from Ronald Weich, Assistant Attorney General, to Senator Harry Reid, Senate Majority Leader, April 29, 2011, http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

[43] John Solomon and Carrie Johnson, "FBI Broke Law for Years to Get Phone Records," *Washington Post,* January 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/18/AR2010011803982.html?wprss=rss_nation. (Hereafter: Solomon and Johnson, "FBI Broke Law.") NSLs are authorized under five federal statutes. (1) Under the Electronic Communications Privacy Act (18 U.S.C. § 2709), the FBI can obtain subscriber information for telephone and electronic communication as well as toll billing information and electronic communication transaction records. According to FBI information from 2007, this is the NSL authority most frequently used by the agency. (2) Under the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(5)) the FBI can obtain records from financial institutions. This NSL authority is used in investigations of potential terror financing. (3) Under the Fair Credit Reporting Act (15 U.S.C. §§ 1681u), the FBI can obtain from credit reporting agencies (a) the names of financial institutions with which the subject of the NSL has an account and (b) consumer identifying information. (4) Also under the Fair Credit Reporting Act (15 U.S.C. §1681v), the FBI can obtain a full credit report—15 U.S.C. §1681v was added by the PATRIOT Act. (5) Under the National Security Act (50 U.S.C. § 436) the FBI can obtain a variety of records related to the finances and travel of government employees. These may be obtained only in investigations involving alleged improper disclosure of classified information by such employees. See CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu, p. 4. (Hereafter: CRS Report R40138.) See also Robert S. Mueller, III, Director, Federal Bureau of Investigation, "Statement Before the Senate Committee on the Judiciary," March 27, 2007, http://www.fbi.gov/news/testimony/the-fbis-use-of-national-security-letters-2.

[44] Ibid, 15 U.S.C. §1681v.

[45] Prior to the PATRIOT Act, the FBI Director or a senior FBI Headquarters official could formally issue NSLs. The PATRIOT Act expands and decentralizes this authority by granting it to FBI field office heads (special agents in charge) as well. See CRS Report R41619, pp. 1-2. See also Solomon and Johnson, "FBI Broke Law."

Currently, the information sought via an NSL "must only be relevant to protecting against international terrorism or clandestine intelligence activities."[46] However, an NSL-related investigation of an American citizen or legal permanent resident cannot be based solely on First Amendment-protected activities.[47]

The implementation of the post-USA PATRIOT Act NSL regimen at the FBI has not been seamless. In 2007, the DOJ Inspector General initially reported that "the FBI used NSLs in violation of applicable NSL statutes, the Attorney General Guidelines, and internal FBI policies," although no evidence was found of criminal misconduct.[48] In a subsequent report in 2008, the Inspector General concluded that DOJ and the FBI "have made significant progress in addressing the need to improve compliance in the FBI's use," but "it is too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified."[49]

Moreover, between 2003 and 2006 some FBI personnel circumvented the NSL process, using crisis conditions as a justification. Namely, in that time period one FBI headquarters unit issued 722 "exigent letters" to obtain telephone toll records for approximately 4,400 telephone numbers in lieu of NSLs. The unit included representatives from three communications service providers. These representatives typically received the exigent letters from FBI employees working alongside them. None of the 722 exigent letters actually described the specific crises that supposedly made them necessary, and in some cases there were no emergencies.[50] The FBI General Counsel at the time, Valerie E. Caproni, stated in congressional testimony that the exigent letters were

> borne out of a misunderstanding of the import of the USA PATRIOT Act's amendments to ECPA [Electronic Communications Privacy Act (18 U.S.C. § 2709)]. For reasons lost in the fog of history—but no doubt partially the result of the intense pace of activity in the months following the 9/11 attacks—the FBI did not adequately educate our workforce that Congress had provided clear mechanisms to obtain records in emergency situations. Although guidance was eventually provided in August 2005, the employees who had been using exigent letters for several years simply did not recognize the applicability of that guidance to their situation.[51]

[46] AALL, *National Security*, p. 1.

[47] CRS Report R41619, p. 2.

[48] U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI Use of National Security Letters,* March 2007, p. 124. http://www.justice.gov/oig/special/s0703b/final.pdf.

[49] U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, March 2008, p. 8, http://www.justice.gov/oig/special/s0803b/final.pdf.

[50] Valerie E. Caproni, General Counsel, Federal Bureau of Investigation, "Statement Before the House Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Civil Liberties," April 14, 2010, http://www2.fbi.gov/congress/congress10/caproni041410.htm. (Hereafter: Caproni, "Statement.") In addition to the 722 letters, 76 other exigent letters were signed by FBI personnel who worked outside of the headquarters unit in question. On the letters, see also U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Information Requests for Telephone Records,* January 2010, pp. 19-21, http://www.justice.gov/oig/special/s1001r.pdf.

[51] Caproni, "Statement."

In March 2007, the FBI ended the use of exigent letters.[52] Regardless, they have played into recent congressional debate regarding the extension of key provisions within the PATRIOT Act.[53]

Debate over Civil Liberties Issues

When the USA PATRIOT Act was signed into law, then-Attorney General John Ashcroft said

> Law enforcement is now empowered with new tools and resources necessary to disrupt, weaken, and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish the perpetrators of terrorist acts.... The American people can be assured law enforcement will use these new tools to protect our nation while upholding the sacred liberties expressed in the Constitution.[54]

And FBI Director Mueller has testified to Congress that "the USA PATRIOT Act has changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act."[55]

But others were concerned about the constitutional implications of the USA PATRIOT Act. Law Professor Susan Herman notes that four of the provisions described above[56] "exemplify several different ways in which the USA PATRIOT Act allow the executive branch to deviate from the presumptive Fourth Amendment[57] model requiring: (1) some form of individualized suspicion (presumptively probable cause), (2) antecedent judicial review where feasible, and (3) notice of any search."[58]

After passage of the act, the Electronic Freedom Foundation worried that "the civil liberties of ordinary Americans have taken a tremendous blow with this law, especially the right to privacy in our online communications and activities."[59] The Rutherford Institute argued that while the USA PATRIOT Act "may not have been designed to restrict American citizens' civil liberties, its unintended consequences threaten the fundamental constitutional rights of people who have absolutely no involvement with terrorism."[60] And the American Civil Liberties Union (ACLU)

---

[52] Ibid.

[53] For more information, see CRS Report R40138.

[54] *The USA Patriot Act Background Report*, PBS Newshour, March 27, 2006, http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/patriotact.html. (Hereafter: PBS Newshour, March 27, 2006.)

[55] U.S. Congress, Senate Committee on the Judiciary, *Sunset Provisions of the USA Patriot Act*, Testimony of Robert Mueller, Director, FBI, 109th Cong., 1st sess., April 5, 2005.

[56] P.L. 107-56, §213, §215, §218, and §505.

[57] The Fourth Amendment to the U.S. Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[58] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," *Harvard Civil Rights-Civil Liberties Law Review,* Vol. 41, No. 1, Winter 2006, pp. 70-1.

[59] Electronic Freedom Foundation (EFF), *EFF Analysis Of The Provisions Of The USA PATRIOT Act*, October 31, 2011, http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.

[60] John W. Whitehead and Steven H. Aden, "Forfeiting 'Enduring Freedom' for 'Homeland Security;' A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives," *American University Law Review,* Vol. 51, October 2002, p. 1083, http://www.wcl.american.edu/journal/lawrev/51/correctedaden.pdf?rd=1.

charges that "the mammoth USA PATRIOT Act expanded government powers in ways that will diminish liberty for years to come."[61] They specifically note that the wiretapping and intelligence provisions of the act "minimize the role of a judge in ensuring that law enforcement wiretapping is conducted legally and with proper justification, and they permit use of intelligence investigative authority to by-pass normal criminal procedures that protect privacy."[62]

In 2005, debate over the USA PATRIOT Act resumed when Congress deliberated extension of certain provisions of the act that were scheduled to expire (sunset). Eventually, Congress passed, and on March 9, 2006, President Bush signed into law, an extension of several of the USA PATRIOT Act provisions that provided the FBI with additional authorities.[63] In its legislation, Congress added new civil liberties protections. For example, in the case of requests to the FISA Court for an order to obtain business records, government agents are now required to present the court with data proving how the evidence sought will apply to the relevant investigation.[64] The reauthorizing legislation also afforded greater protections for library, medical, and educational records and provides the party forced to disclose the business information the right to seek the advice of an attorney.[65]

In 2011, Congress again considered the extension of three expiring amendments to FISA. Two of these were enacted as part of the USA PATRIOT Act—the "roving wiretap" and "business records" provisions. The third amendment was enacted in 2004 as part of the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). Known as the "lone wolf" provision, it permits surveillance of non-U.S. persons engaged in, or preparing to engage in, international terrorism without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

In arguing for extension of these provisions before the House of Representatives, law professor Nathan Sales testified that "they simply let counterintelligence agents use some of the same techniques that ordinary criminal investigators have been using for decades – techniques that federal courts repeatedly have upheld."[66] At the same hearing, Acting Assistant Attorney General Todd Hinnen added, "Robust substantive standards and procedural protections are in place to ensure that these tools are used responsibly and in a manner that safeguards Americans' privacy and civil liberties."[67]

---

[61] American Civil Liberties Union (ACLU), *Insatiable Appetite: The Government's Demand for New and Unnecessary Powers After September 11*, updated October 2002, p. 10, http://www.aclu.org/files/FilesPDFs/insatiable%20appetite%20final.pdf.

[62] ACLU Legislative Analysis, "USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances," November 1, 2001, http://www.ratical.org/ratville/CAH/l110101a.html.

[63] These are contained in the USA PATRIOT Improvement and Reauthorization Act of 2005 (P.L. 109-177) and the USA PATRIOT ACT Additional Reauthorizing Amendments Act of 2006 (P.L. 109-178).

[64] See 50 U.S.C. 1861(b)(2).

[65] See 50 U.S.C. 1861(a)(3) and 50 U.S.C. 1861(d)(1)(B).

[66] U.S. Congress, House Committee on the Judiciary, *Statement of Nathan A. Sales, Assistant Professor of Law, George Mason University School of Law,* The Reauthorization of the PATRIOT Act Hearing, 112th Cong., 1st sess., March 9, 2011, p. 1, http://judiciary.house.gov/hearings/pdf/Sales03092011.pdf.

[67] Ibid, *Statement of Todd M. Hinnen, Acting Assistant Attorney General, Department of Justice,* p. 4, http://judiciary.house.gov/hearings/pdf/Hinnen03092011.pdf.

Congress passed legislation, S. 990, to extend the provisions until June 1, 2015, and President Obama signed the legislation (P.L. 112-14) on May 26, 2011.[68]

Revised Attorney General Guidelines

The FBI and DOJ also emphasized their forward-leaning approach with the September 29, 2008, revision of the *Attorney General's Guidelines for Domestic FBI Operations*,[69] which they claim "make the FBI's operations in the United States more effective by providing simpler, clearer, and more uniform standards and procedures."[70] Referred to as the "Mukasey Guidelines" after Michael B. Mukasey, who was Attorney General at the time of their release, this is the latest in a series of guidelines stretching back to 1976 that govern the FBI's investigative activities.[71] The Mukasey Guidelines went into effect on December 1, 2008. In large part, these guidelines sprang from the post-9/11 national security context, in which the FBI surmised that it could not simply react to crimes. It had to preemptively search for criminal, counterintelligence, and terrorist threats to the homeland.[72] As the FBI's General Counsel stated in congressional testimony:

> We believe that this will allow the FBI to take additional necessary steps to becoming a more proactive organization. One of the key issues that we think the FBI needs to be able to do is assess potential risks and vulnerabilities. Having these additional techniques available at the assessment level, we think, will be key to the FBI's ability to efficiently and effectively answer those questions and assess risks.[73]

The 2008 revision to the guidelines represents a consolidation of several other previously stand-alone documents that had governed FBI investigations. Also a work in progress is the 2008 *Domestic Investigations and Operations Guide* (DIOG)—the FBI's document governing the agency's implementation of the Mukasey Guidelines—which the FBI modified in 2011.[74]

---

[68] For more information, see CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

[69] Available at http://www.ignet.gov/pande/standards/prgexhibitg1.pdf.

[70] U.S. Department of Justice, "Memorandum for the Heads of Department Components: The Attorney General's Guidelines for Domestic FBI Operations," press release, September 29, 2008, http://www.justice.gov/ag/readingroom/guidelines-memo.pdf.

[71] See Emily Berman, *Domestic Intelligence: New Powers, New Risks,* Brennan Center for Justice at New York University School of Law, 2011, pp. 8-9, 11. (Hereafter: Berman, *Domestic Intelligence.*)

[72] Prepared Statement of Elisebeth Collins Cook, Assistant Attorney General, Office of Legal Policy, DOJ, and Valerie Caproni, General Counsel, FBI, U.S. Congress, Senate Select Committee on Intelligence, *Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence*, 110th Cong., 2nd sess., September 23, 2008, S. HRG. 110–846 (Washington: GPO, 2009), p. 10, http://intelligence.senate.gov/pdfs/110846.pdf.

[73] U.S. Congress, Senate Select Committee on Intelligence, Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence, 110th Cong., 2nd sess., September 23, 2008, S. HRG. 110–846 (Washington: GPO, 2009), p. 17, http://intelligence.senate.gov/pdfs/110846.pdf. (Hereafter: Hearing, "Attorney General Guidelines.")

[74] Department of Justice, Office of the Inspector General, Oversight and Review Division, *Investigation of Allegations of Cheating on the FBI's Domestic Investigations and Operations Guide (DIOG) Exam,* Washington, DC, September 2010, pp. 1, 34, http://www.justice.gov/oig/special/s100927.pdf. Interestingly, this report discusses the findings of an investigation into a string of incidents in which FBI employees cheated on a mandatory exam covering the DIOG. DIOG, redacted, p. 2. For a description of the most recent changes to the DIOG, see Charlie Savage, "FBI Agents Get Leeway to Push Privacy Bounds," *New York Times,* June 12, 2011, http://www.nytimes.com/2011/06/13/us/13fbi.html?_r=1.

The most prominent changes in the Mukasey Guidelines and the DIOG concern "assessments." Agents and analysts may now use assessments outside of the more traditional preliminary and full investigations, which require some level of factual predication.[75] Preliminary investigations can be opened with "'allegation or information' indicative of possible criminal activity or threats to the national security." Opening a full investigation requires an "'articulable factual basis' of possible criminal or national threat."[76] On the other hand, opening an assessment does not require allegations, information of possible criminal activity or threat, or an articulable factual basis.[77] Instead, assessments are to follow a specifically articulated purpose, of which there are six:[78]

- check leads on individuals or activities,
- check leads on groups or organizations,
- collect information to analyze potential threats and vulnerabilities,
- gather information for intelligence analysis or planning,
- vet and manage the agency's confidential human sources (informants), and
- collect foreign intelligence.

Assessments are not to be based on "arbitrary or groundless speculation, nor can an assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject."[79] Assessments offer terrorism investigators a variety of techniques, including public surveillance and the use of confidential informants to penetrate conspiracies.[80]

The Bureau has incorporated assessments into its investigative processes. According to numbers made publicly available in March 2011, between December 2008 and March 2009 the FBI initiated 11,667 assessments to check leads on individuals, activities, groups, or organizations. These, in turn, led to 427 preliminary or full investigations. Officials noted that about one-third of the assessments resulted from vague tips.[81] Reportedly, between March 2009 and March 2011, the Bureau opened 82,325 assessments. About half of the assessments from this time frame

[75] Hearing, "Attorney General Guidelines," p. 17.

[76] DIOG, redacted, pp. 76, 85.

[77] According to the DIOG, "Although difficult to define, 'no particular factual predication' is less than 'information or allegation' as required for the initiation of a preliminary investigation. For example, an assessment may be conducted when there is a basis to know: (i) whether more information or facts are required to determine if there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. Regardless of whether specific approval or specific documentation is required, an FBI employee should be able to explain the purpose of an assessment and the reason for the methods used to conduct the assessment. Those FBI employees who conduct assessments are responsible for assuring that assessments are not pursued for frivolous or improper purposes and are not based solely on First Amendment activity or on the race, ethnicity, national origin, or religion of the subject of the assessment." DIOG, redacted, p. 39.

[78] DIOG, redacted, pp. 44-56. See also, Andrew Kalloch, "FBI General Counsel Defends New Guidelines," *Harvard Law Record,* December 4, 2008, updated September 29, 2009, http://www.hlrecord.org/2.4463/fbi-general-counsel-defends-new-guidelines-1.577396.

[79] DIOG, redacted, p. 39.

[80] Charlie Savage, "Wider Authority for F.B.I. Agents Stirs Concern," *New York Times,* October 29, 2009.

[81] Charlie Savage, "F.B.I. Casts Wide Net Under Relaxed Rules for Terror Inquiries, Data Show," *New York Times*, March 26, 2011, http://www.nytimes.com/2011/03/27/us/27fbi.html?_r=2&sq=savage&st=cse&scp=3&pagewanted=print. (Hereafter: Savage, "F.B.I. Casts.")

focused on determining whether specific groups or individuals were spies or terrorists. This pool of 42,888 assessments produced just under 2,000 full or preliminary investigations.[82]

Critics have voiced broad concerns about the Mukasey Guidelines. One detailed study has noted that they "tip the scales too far in favor of relatively unchecked government power, allowing the FBI to sweep too much information about too many innocent people into the government's view. In so doing, they pose significant threats to Americans' civil liberties and risk undermining the very counterterrorism efforts they are meant to further."[83]

According to media reports, Farhad Khera, executive director of the nonprofit Muslim Advocates, has suggested that the Attorney General Guidelines are invasive and based on "generalized suspicion and fear on the part of law enforcement, not on individualized evidence of criminal activity."[84] The ACLU also criticized the large number of assessments the FBI appears to be initiating. A policy counsel with the civil liberties group noted that the large number of assessments that did not lead to preliminary or full investigations are "against completely innocent people that are now bound up within the FBI's intelligence system forever."[85] The FBI's General Counsel viewed the numbers from a more proactive investigative posture: "Recognize that the FBI's policy—that I think the American people would support—is that any terrorism lead has to be followed up."[86]

Under the Freedom of Information Act, in late July 2010 the ACLU requested information from the FBI regarding the agency's amassing of racial and ethnic data based on the new guidelines.[87] As written, the guidelines allow for the collection of information about ethnic or racial communities and justify the gathering of such information for proactive purposes. The DIOG states that it should be done if it "will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness for the purpose of performing intelligence analysis."[88]

Joint Terrorism Task Forces (JTTFs)

JTTFs are locally based, multi-agency teams of investigators, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes. Seventy-one of the 106 JTTFs currently operated by DOJ and the FBI were created since 9/11. Over 4,400 federal, state, and local law enforcement officers and agents—more than four times the pre-9/11 total—

[82] Charlie Savage, "F.B.I. Focusing on Security Over Ordinary Crime," *New York Times,* August 23, 2011, http://www.nytimes.com/2011/08/24/us/24fbi.html.

[83] Berman, *Domestic Intelligence,* p. 1.

[84] Brent Jones, "ACLU Seeks Information About FBI Racial, Ethnic Data Collection," *Baltimore Sun,* July 28, 2010, http://articles.baltimoresun.com/2010-07-28/news/bs-md-aclu-fbi-20100728_1_ethnic-data-profiling-aclu-representatives; Pete Yost, "FBI Defends Guidelines on Eve of Senate Testimony," *Associated Press,* cited in boston.com, July 27, 2010, http://www.boston.com/news/nation/washington/articles/2010/07/27/fbi_defends_guidelines_on_eve_of_senate_testimony/. (Hereafter: Yost, July 27, 2010.)

[85] Savage, "F.B.I. Casts."

[86] Ibid.

[87] Yost, July 27, 2010.

[88] DIOG, redacted, p. 32.

work in them. These officers and agents come from more than 600 state and local agencies and 50 federal agencies.[89]

The FBI considers the JTTFs "the nation's front line on terrorism."[90] They "investigate acts of terrorism that affect the U.S., its interests, property and citizens, including those employed by the U.S. and military personnel overseas."[91] As this suggests, their operations are highly tactical and focus on investigations, developing human sources (informants), and gathering intelligence to thwart terrorist plots.

JTTFs also offer an important conduit for the sharing of intelligence developed from FBI-led counterterrorism investigations with outside agencies and state and local law enforcement. To help facilitate this, especially as the threat of homegrown jihadists has emerged, the number of top-secret security clearances issued to local police working on JTTFs has increased from 125 to 878 between 2007 and 2009.[92]

There is also a National JTTF, which was established in July 2002 to serve as a coordinating mechanism with the FBI's partners. Some 40 agencies are now represented in the National JTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners.[93]

Intelligence Reform

The 9/11 terrorist attacks have been called a major intelligence failure.[94] In response to criticisms of its intelligence capabilities, the FBI over the last decade has introduced a series of reforms

[89] Federal Bureau of Investigation, "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

[90] Federal Bureau of Investigation, "Protecting America Against Terrorist Attack: A Closer Look at Our Joint Terrorism Task Forces," May 2009, http://www.fbi.gov/page2/may09/jttfs_052809.html.

[91] Brig Barker and Steve Fowler, "The FBI Joint Terrorism Task Force Officer," *The FBI Law Enforcement Bulletin*, vol. 77, no. 11 (November 2008), p. 13.

[92] Kevin Johnson, "FBI Issues More Top Secret Clearance for Terrorism Cases," USA Today, August 12, 2010, http://www.usatoday.com/news/nation/2010-08-12-secret-clearances_N.htm; STRATFOR, A Decade of Evolution in U.S. Counterterrorism Operations, Special Report, December 2009, http://www.stratfor.com/memberships/150745/analysis/20091216_us_decade_evolution_counterterrorism_operations?ip_auth_redirect=1; CRS Report RL33033, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*, by Alfred Cumming.

[93] DOJ, "Joint Terrorism Task Force," http://www.justice.gov/jttf/.

[94] There is a large body of literature on the failures associated with the attacks of September 11, 2001, and broader issues associated with the effectiveness of the Intelligence Community in general. According to William E. Odom, *Fixing Intelligence for a More Secure America* (New Haven, CT: Yale University Press, 2003), p. 187, the attacks of 9/11 represent a failure of both intelligence and policy. See also *The Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: Report to the President of the United States*, March 31, 2005. (Hereafter cited as WMD Report.) Chapter 10 of this report, "Intelligence at Home: The FBI, Justice, and Homeland Security," is the most germane with respect to FBI intelligence reform. See also Senate Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Pre-War Intelligence Assessments on Iraq*, July 7, 2004. See also the National Academy of Public Administration, *Transforming the FBI: Progress and Challenges,* January 2005. Chapter 3 on Intelligence is most pertinent to the topic of this CRS report. See also Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Palo Alto, CA: Hoover Institution, Stanford University, 2005); U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks,* November 2004, recently released in redacted form.

intended to transform the agency from a largely reactive law enforcement agency focused on criminal investigations into a more proactive, agile, flexible, and intelligence-driven[95] agency that can prevent acts of terrorism.[96]

Robert S. Mueller III, who became the FBI Director just prior to the 9/11, has vowed to assert headquarters' control over the FBI's historically fragmented and much-criticized intelligence program. He signaled his intention to improve the FBI's intelligence program by consolidating and centralizing control over intelligence capabilities, both at FBI Headquarters and in the FBI's largely autonomous field offices.[97] He has contended that intelligence has always been one of the FBI's core competencies,[98] organic to the FBI's investigative mission,[99] and he asserted that the organization's intelligence efforts have been and will continue to be disciplined by the intelligence cycle (i.e., the development and conduct of intelligence collection requirements, collection, analysis, and dissemination).

Since the 2001 attacks, Director Mueller has instituted a number of reforms. He created a new Directorate of Intelligence (DI) at headquarters. He also acted on a recommendation by the Weapons of Mass Destruction Commission and established a National Security Branch at headquarters which integrated the FBI's Counterterrorism and Counterintelligence Divisions with the DI, the Weapons of Mass Destruction Directorate, and the Terrorist Screening Center.[100]

More fundamentally, perhaps, Director Mueller established Field Intelligence Groups (FIGs), which could be viewed as a cornerstone of his reforms, at each of the FBI's 56 field offices in an effort to improve the agency's intelligence capacity by combining its intelligence and investigative capabilities. FIGs are comprised of agents, analysts, linguists, and surveillance specialists. A FIG's principal mission is to identify intelligence gaps, obtain and analyze raw intelligence from FBI investigations and sources, and generate intelligence products and disseminate them to the intelligence and law enforcement communities in order to help guide investigations, programs, and policy. Arguably, the mission of the FIGs is nothing less than to "drive," or inform the direction of, the FBI's counterterrorism effort by identifying, assessing, and attacking emerging threats "before they flourish."[101]

Intelligence Information Reports (IIRs) are a primary component of the FBI's post-9/11 transformation. FIGs disseminate IIRs.[102] These reports are formatted as teletype messages and

[95] For purposes of this report, intelligence is defined to include foreign intelligence, counterintelligence, and criminal intelligence. Experts differ on the extent to which there may be a synergy between traditionally defined foreign intelligence and criminal intelligence. One's perspective on the relationship between the law enforcement and intelligence disciplines can have direct effects on policy preferences, including the role of the FBI in domestic intelligence, and domestic intelligence resource allocation strategies.

[96] P.L. 108-447; the FY2005 Consolidated Appropriations Act provided the FBI with additional human resource tools for recruitment and retention, including authority to provide retention and relocation bonuses to certain categories of FBI employees, and the establishment of an FBI Investigative Reserve Service.

[97] See statement of Robert S. Mueller, III, Director, FBI, in U.S. Congress, House Committee on Appropriations, Subcommittee on the Departments of Commerce, Justice, State, the Judiciary and Related Agencies, June 18, 2003.

[98] Core competencies are defined as a related group of activities central to the success, or failure, of an organization. In the private sector, core competencies are often the source of a company's competitive advantage. See C. K. Prahalad and Gary Hamel, "The Core Competency of the Corporation," *Harvard Business Review*, April 1, 2001.

[99] See statement of Robert S. Mueller, III, Director, FBI, in U.S. Congress, Senate Judiciary Committee, July 23, 2003.

[100] FBI, *National Security Branch*, http://www.fbi.gov/about-us/nsb.

[101] See statement of Robert S. Mueller, Director, FBI, in U.S. Congress, Senate Judiciary Committee, March 25, 2009.

[102] Known as "direct dissemination," this is a transformation of a post-9/11 FBI policy that centralized IIR (continued...)

shared electronically with the law enforcement and intelligence communities. They contain "raw" intelligence—"unevaluated intelligence information, generally from a single source, that has not fully been evaluated, integrated with other information, or interpreted and analyzed."[103] These reports include information "extracted" from FBI case files.[104] The agency emphasizes that the information in IIRs must not be "based solely on the exercise of First Amendment protected activities, or on the race, ethnicity, national origin, or religion of the subject."[105] In 2010, the FBI produced over 25,000 IIRs, which included counterintelligence, counterterrorism, and criminal information as well as information related to cyber issues and weapons of mass destruction.[106]

In making intelligence a priority, Director Mueller also adopted a Strategy Management System, establishing a Strategic Execution Team (SET) to execute organizational changes and to build support and momentum for institutional change across the Bureau.[107] Mueller testified in 2008, "we established Strategic Execution Teams to help us assess our intelligence program, evaluate best practices, decide what works and what does not work, and to standardize it throughout the FBI. The purpose of the SET is to accelerate improvements to our intelligence capabilities, to ensure we are an intelligence-driven organization and to drive a change in mindsets throughout the FBI."[108]

More specifically, the FBI acted on SET recommendations and restructured the FIGs in each of its field offices to conform to one model, based on best practices from the field, and adapted to the size and complexity of each office. As a result, according to Director Mueller, FIG-Headquarter coordination has improved. In 2008, Mueller told Congress that another result of the

(...continued)

dissemination from headquarters. "In 2010, the FBI continued to adjust its intelligence dissemination practices. During the early years of the FBI Directorate of Intelligence, intelligence reporting was prepared by the Field Intelligence Groups in each of the FBI's Field Offices, and was then sent to FBI Headquarters in Washington, DC, for review and editing prior to dissemination. This was necessary to ensure consistency and quality in the raw reporting that the FBI provided to other parts of the Federal Government, as well as to its State, local, tribal, and foreign partners. However, in 2009 the Bureau determined that its raw intelligence reporting had reached a state of maturity that justified direct dissemination of intelligence reporting. The FBI accelerated its original timetable and, in March 2010, authorized all 56 field offices to directly disseminate most intelligence information reports (IIRs) to its Intelligence Community and law enforcement partners. While the FBI continues to disseminate its analytic intelligence reports centrally, a new dissemination team was added to the Directorate of Intelligence to improve efficiencies in sharing analytic intelligence with its partners and customers." See Federal Bureau of Investigation, *FBI Information Sharing Report, 2010,* p. 3, http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/fbi-information-sharing-report-2010. (Hereafter: Federal Bureau of Investigation, *FBI Information.)*

[103] Request for Records Disposition Authority, Standard Form 115, Job Number n1-065-10-25, National Archives and Records Administration, December 14, 2010, http://207.245.165.90/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-025_sf115.pdf; Interagency Threat Assessment and Coordination Group, *Intelligence Guide for First Responders*, p. 30, http://www.nctc.gov/docs/itacg_guide_for_first_responders.pdf.

[104] Ibid.

[105] Federal Bureau of Investigation, *FBI Information, p. 21.*

[106] Ibid, p. 22.

[107] See U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, 112th Cong., 1st sess., February 2011, p. 53, http://hsgac.senate.gov/public/_files/Fort_Hood/FortHoodReport.pdf. (Hereafter: *A Ticking Time Bomb.*)

[108] U.S. Congress, House Committee on the Judiciary, Statement of Robert S. Mueller, III, Director, FBI, 110th Cong., 2nd sess., September 16, 2008.

single-model standardized FIG approach is that special agents and analysts are now able to transition more easily and quickly from one field office FIG to another.[109]

Reform Initiatives: A Work in Progress

Recently, post-9/11 intelligence reform at the FBI has been critiqued by the Senate Committee on Homeland Security and Governmental Affairs (HSGAC). Its February 2011 report, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, paints a mixed picture regarding FBI efforts to integrate intelligence with investigative operations.[110] According to the committee's report, which focuses on the counterterrorism lessons derived from the U.S. government's failure to prevent the November 2009 shootings at Fort Hood, there is no question that the FBI has made substantial progress since 9/11 and has achieved many successes in countering terrorism as a result of FBI Director Mueller's leadership.[111] However, it remains unclear whether the FBI has truly transformed into an "intelligence-driven" organization, meaning that the analysis, production, and exploitation of intelligence is not simply yoked to the process of investigating cases en route to prosecution. In essence, in an intelligence-driven organization, "intelligence is a preeminent objective separate from whether a prosecution occurs."[112]

Others have echoed *A Ticking Time Bomb's* appraisal. In an April 2011 letter to Attorney General Eric H. Holder and Director of National Intelligence James R. Clapper, Jr., the FBI Intelligence Analysts Association (FBI IAA) criticized the efforts the agency has made toward becoming "intelligence-driven."[113] The letter stated that

> the Bureau has not yet fully established intelligence analysis as a core mission of the organization. Rather than being a driver of operational activity, intelligence is still typically seen as an enabler to the law enforcement mission. Intelligence is often viewed as an operational asset, an additional tool that can be used much in the same way that technology can be used to help investigate cases. But to be "intelligence-driven" in the FBI cannot mean intelligence should be a surrogate or a component of the law enforcement mission. America's security requires that FBI operations be guided by the best possible assessment of the threat. Intelligence must drive operations by identifying threats and vulnerabilities based on our nation's criminal and national security concerns.[114]

[109] Ibid.

[110] *A Ticking Time Bomb*. The report discusses findings from an investigation into the failure of the U.S. government to stop U.S. Army Major Nidal Hasan's alleged mass shooting at Fort Hood, TX, in November 2009. It claimed 13 lives. Forty-three people were injured in this attack as well.

[111] See *A Ticking Time Bomb*, p. 51.

[112] Ibid, p. 54.

[113] The FBI IAA used the letter to lay out what it sees as key traits for the next FBI director. The key traits included the following: "Trait one: the next Director must have a deep understanding of and commitment to both the intelligence and law enforcement mission of the Bureau.... Trait two: the next Director must strengthen a culture of collaboration within the FBI and across the USIC and continue building the FBI intelligence career service.... Trait three: the next Director must be a seasoned manager of a global enterprise who can lead a group of diverse professionals—agents, intelligence analysts, and other FBI employees—and form strong partnerships to achieve the FBI's mission." See Letter from Clarence A. Stiehm II, President, FBI Intelligence Analysts Association, to James R. Clapper, Jr., Director of National Intelligence, and Eric H. Holder, United States Attorney General, April 5, 2011, http://www.fbiiaa.org/wp-content/uploads/2011/04/FBI_IAA_letter_to_DNI_Clapper_and_AG_Holder.pdf.

[114] Ibid.

One of the Bureau's latest innovations regarding the integration of intelligence and operations is the "Fusion Cell Concept." It appears to feature intelligence as a component of the law enforcement mission by blending interagency information sharing with targeting within the FBI's counterterrorism division. As described by a senior FBI counterterrorism official, the Fusion Cell Concept "take[s] a *target-centric* [emphasis added] approach to the threat by combining FBI and Intelligence Community tactical analysis, strategic analysis, and operational capabilities to identify and mitigate the priority threats."[115] The FBI uses "intelligence generated from these Fusion Cells to strategically select targets posing the greatest threat."[116] The FBI's public rhetoric about "Fusion Cells" stresses proactivity, but it remains unclear how this substantially differs from the type of work that is supposed to occur in task force settings such as JTTFs.

However, the FBI IAA has stated that analysts at the FBI continue to be relegated to "support" roles[117] (i.e., they react to direction from special agents rather than being full partners in an intelligence-driven investigative operation). They argue that intelligence analysts should have professional parity with special agents to rapidly reform the FBI's institutional culture. The FBI IAA's indictments of the agency's efforts come from insiders working on intelligence matters within the FBI. However, it must be kept in mind that these same individuals publicly lobby on behalf of FBI intelligence analysts.[118]

A Ticking Time Bomb also emphasized that the necessary transformation of the FBI is incomplete, and "we must be impatient for progress."[119] Specifically, the committee cited the Fort Hood shootings as a warning that the FBI's transformation remains a work in progress and that the FBI must accelerate efforts—especially given the growing complexity and diversity of the homegrown terrorist threat.[120] Among its findings, the committee said that the FBI's Hassan inquiry was impeded by division among the agency's field offices, insufficient use of intelligence analysis, outdated tradecraft, and poor coordination within the JTTFs and between the JTTFs and headquarters.[121] As a counterpoint, the HSGAC report cited the case of the terrorist plot by Najibullah Zazi to attack the New York City subway system in September 2009 as an FBI success, noting that the coordination across federal, state, and local departments, led by two JTTFs, was excellent and unprecedented.[122]

Terrorism Prevention and Proactive Investigations

One observer has described intelligence gathering by the FBI in the post-9/11 context as "driven by a theory of preventive policing: in order to anticipate the next terror attack, authorities need to track legal activities…. It focuses not on crime, but on the possibility that a crime might be

[115] Mark F. Giuliano, Assistant Director, FBI Counterterrorism Division, *The Post 9/11 FBI: The Bureau's Response to Evolving Threats,* Statement for the Record at The Washington Institute for Near East Policy, Stein Program on Counterterrorism and Intelligence, April 14, 2011, p. 5.

[116] Ibid.

[117] FBI Intelligence Analysts Association, *Intel Shift "Needs To" Happen,* February 26, 2010.

[118] The FBI IAA describes itself as an "independent advocate representing the professional interests, both internally and externally" of the FBI's intelligence analysts. See http://www.fbiiaa.org/.

[119] *A Ticking Time Bomb*, p. 51.

[120] Ibid, p. 52.

[121] Ibid, pp. 55-56.

[122] Ibid, p. 55.

committed at some future date."[123] This preventative stance can be seen in an intelligence-gathering operation related to recent events in Libya. The FBI has interviewed more than 800 Libyans residing in the United States to determine if there is any threat of terror attacks against American targets because of U.S. military action in Libya.[124] During congressional testimony, Director Mueller stated that the FBI wanted to make certain that "we are on guard with the possibility of terrorist attacks emanating somewhere out of Libya."[125]

This proactive posture also involves challenges for the agency—especially in determining when individuals move from radical activity involving First Amendment-protected behavior to violent extremism.[126] Because not all terrorist suspects follow a single radicalization roadmap on their way to executing plots, U.S. law enforcement also faces the task of discerning exactly when radicalized individuals become real threats.

As suggested, timing is everything. To preemptively stop terrorists, law enforcement requires accurate and timely intelligence. The FBI generates terrorism cases from a number of sources. Information about terrorist threats or suspicious incidents is brought to the attention of the FBI by the public; other government agencies (particularly those in the intelligence community); state and local law enforcement; ongoing FBI investigations (including sources, surveillance, financial analysis,[127] and tactical analysis); and FBI Legal Attachés stationed abroad. Most FBI investigations develop from information or leads generated by pre-existing FBI investigations, or casework and liaison with other federal agencies or international counterparts. A handful of leads stem from information generated by local or state law enforcement and filtered up to the FBI via intelligence fusion centers.[128]

To counter violent plots, U.S. law enforcement has employed two tactics that have been described by one scholar as the "Al Capone"[129] approach and the use of "agent provocateurs."[130] The

[123] Thomas Cincotta, "From Movements to Mosques, Informants Endanger Democracy," *The Public Eye*, Summer 2009, http://www.publiceye.org/magazine/v24n2/movements-to-mosques.html. (Hereafter: Cincotta, "From Movements to Mosques.")

[124] Richard Esposito and Jason Ryan, "FBI Has Interviewed 800 Libyans About Terror Threat," *abcnews.com*, April 7, 2011, http://abcnews.go.com/Blotter/fbi-interviewed-800-libyans-terror-threat/story?id=13321227.

[125] Justin Blum, "FBI Monitoring Possibility of Terrorist Attacks From Libya," *Bloomberg*, April 6, 2011, http://www.bloomberg.com/news/2011-04-06/fbi-monitoring-possibility-of-terrorist-attacks-from-libya.html. This wave of interviews mirrors a 2002-2003 effort by the FBI to interview Iraqis living in America as the Iraq war began. See Devlin Barrett, "FBI Questioning Libyans," *Wall Street Journal*, April 5, 2011, http://online.wsj.com/search/term.html?KEYWORDS=DEVLIN+BARRETT&bylinesearch=true.

[126] Eileen Sullivan and Devlin Barrett, "Recent Cases Show Challenge of US Terrorists," *Associated Press*, cited in abcnews.com, March 17, 2010, http://abcnews.go.com/Politics/wireStory?id=10121734.

[127] For example, the FBI's Terrorism Financing Operations Section (TFOS) "coordinates efforts to track and shut down terrorist financing and to exploit financial information in an effort to identify previously unknown terrorist cells and recognize potential activity/planning." Federal Bureau of Investigation, *Today's FBI: Facts and Figures, 2010-2011,* http://www.fbi.gov/stats-services/publications/facts-and-figures-2010-2011/facts-and-figures-2010-2011-pdf.

[128] Dana Priest and William M. Arkin, "Monitoring America," *Washington Post,* December 20, 2010; http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/. (Hereafter Priest and Arkin, "Monitoring.") For background on state and local fusion centers, see CRS Report RL34070, *Fusion Centers: Issues and Options for Congress*, by John Rollins.

[129] Al Capone was a Prohibition-era gang leader engaged in a variety of criminal activities including racketeering, bootlegging liquor, prostitution, and bribery of government officials. He was, however, ultimately arrested and convicted of tax evasion, for which he served an 11-year prison sentence.

[130] Lorenzo Vidino, "Homegrown Jihadist Terrorism in the United States: A New and Occasional Phenomenon?" *Studies in Conflict and Terrorism*, vol. 32, no. 1, January 2009, p. 13, http://pdfserve.informaworld.com/
(continued...)

Capone approach involves apprehending individuals linked to terrorist plots on lesser, non-terrorism-related offenses such as immigration violations.[131] In agent provocateur cases—often called sting operations—government undercover operatives befriend suspects and offer to facilitate their activities. As the "Al Capone" moniker suggests, historically these tactics have been employed against many types of targets such as mafia bosses, white-collar criminals, and corrupt public servants. While these techniques combined with the cultivation of informants as well as surveillance (especially in and around mosques) may be effective in stymieing rapidly developing terrorist plots, their use has fostered concern within U.S. Muslim communities.[132]

The Capone Approach

As mentioned, the Capone approach involves apprehending individuals linked to terrorist plots on lesser, non-terrorism-related offenses such as immigration violations. This approach fits within a preventative mode of counterterrorism prosecution.[133] Experts have noted that immediately after 9/11, DOJ often leveled lesser charges against terrorist suspects to preemptively squelch potential attacks. The author of a 2011 book about the FBI and counterterrorism reported, "of the 417 terrorism indictments in the five years after 9/11 … only 143 of the individuals were actually indicted on specific terrorism charges; the rest were the result of what then-Attorney General Ashcroft called the 'spitting-on-the-sidewalks' approach: driver's license fraud, marriage fraud, wire fraud, immigration violations, and the myriad of other lesser charges that served to disrupt potential plots and get suspects off the streets."[134]

However, according to the Center on Law and Security at New York University School of Law, DOJ has moved toward trying suspected terrorists *as terrorists* instead of leaning heavily on lesser charges: "77% of cases [between September 11, 2009, and September 11, 2010] carried terrorism or national security charges, an increase of nearly 50% compared to the average over the previous eight years."[135] Regardless, the Capone approach is still used in terrorism cases.

Lying to an FBI Special Agent is a charge reminiscent of the Capone approach.[136] A recent example stands out.[137] On July 21, 2010, Paul Rockwood, Jr., a U.S. citizen and Muslim convert, pled guilty to making false statements to the FBI. Rockwood's wife, Nadia Rockwood, also pled guilty to making false statements related to her husband's case. By early 2010, while living in

(...continued)

738522_731260637_907926062.pdf.

[131] See Daveed Gartenstein-Ross and Kyle Dabruzzi, "The Al Capone Model of Anti-Terror Policing: How Old Tactics are Countering New Threats," *The Weekly Standard*, April 12, 2007, http://www.weeklystandard.com/Content/Public/Articles/000/000/013/495wvpqo.asp?page=1.

[132] Paul Vitello and Kirk Semple, "Muslims Say F.B.I. Tactics Sow Anger and Fear," *New York Times*, December 17, 2009, http://www.nytimes.com/2009/12/18/us/18muslims.html.

[133] Dan Eggen and Julie Tate, "U.S. Campaign Produces Few Convictions on Terrorism Charges," *Washington Post*, June 12, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/06/11/AR2005061100381.html; Andrew Adams, "FBI's New Approach: Minor Charges Now Stop Terrorism Later," *Lodi News-Sentinel*, June 17, 2005.

[134] Graff, *The Threat Matrix*, pp. 420-421.

[135] The Center on Law and Security, New York University School of Law, *Terrorist Trial Report Card: September 11, 2001-September 11, 2010*, p.2, http://www.lawandsecurity.org/Portals/0/documents/01_TTRC2010Final1.pdf.

[136] 18 U.S.C. § 1001.

[137] For additional examples, see CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera.

King Salmon, AK, Paul Rockwood had developed a list of 15 people he planned to kill, believing that they had desecrated Islam. He had also researched explosives and shared with others ideas about mail bombs or using firearms to kill his targets.[138] It appears that prosecutors did not pursue a case based on more substantive terrorism charges and opted to neutralize a threat—someone apparently preparing to kill people—by using a false statement charge.

Lesser charges against a suspect in a terrorism case may also act as a placeholder until evidence to support a more serious charge is gathered. The utility of this preventative technique coupled with actual terrorism charges was exhibited by the FBI in its case against Najibullah Zazi. He arrived in New York on September 10, 2009, with explosive material and plans to detonate bombs in New York's subway system. Zazi feared authorities had caught up with him and returned to Denver on September 12. Between September 10 and 19, the FBI monitored his activities and bolstered its case with searches of a vehicle and locations linked to him in New York and Denver. Zazi also agreed to interviews with the FBI in Denver. Then, on September 19 FBI special agents arrested Zazi in Aurora, CO, for knowingly and willfully lying to the FBI. Presumably this was done because he might flee. Four days later, a grand jury returned a more substantive one-count indictment against him on weapons of mass destruction charges.[139]

Agent Provocateur Cases

Agent provocateur cases—sting operations—rely on expert determination by law enforcement that a specific individual or group is likely to move beyond radicalized talk and engage in violence or terrorist plotting. The ultimate goal is to catch a suspect committing an overt criminal act such as pulling the proverbial trigger but on a dud weapon. By engaging in such strategy, investigators hope to obtain ironclad evidence against suspects. Although an official count of terrorist sting operations is not publicly available, the FBI has said that of all the terrorist plots disrupted between 9/11 and the September 2009 Zazi plot to bomb the New York City subway, only two plotters were "prepared to move ahead with their plots without the benefit or knowledge of government informants or U.S. officials."[140] Since 2009, according to The Center for Law and Security at the New York University School of Law, the FBI has arrested 41 people on terrorism charges through sting operations.[141]

An FBI investigation exemplifies this approach. On November 26, 2010, Mohamed Osman Mohamud was arrested after he attempted to set off what he believed was a vehicle bomb at an annual Christmas tree lighting ceremony in Portland, OR. Mohamud thought he had plotted with

[138] DOJ Press Release, "Alaska Man Pleads Guilty to Making False Statements in Domestic Terrorism Investigation, Spouse Pleads Guilty to Making False Statements," July 21, 2010, http://www.fbi.gov/anchorage/press-releases/2010/ak072110.htm; Colleen Kelly, "Alaskan Couple in Domestic Terrorism Plot Sentenced," ktva.com (Anchorage, AK), August 23, 2010, http://www.ktva.com/alaskanews/ci_15870578?source=rss.

[139] U.S. Department of Justice, "Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad and Providing Material Support to Al-Qaeda," press release, February 22, 2010, http://www.justice.gov/opa/pr/2010/February/10-ag-174.html; Nicole Vap, "Timeline of Terror Plot Investigation," KUSA TV, NBC affiliate, September 2009, http://www.9news.com/news/specials/terrorplot/article.aspx?storyid=123658&catid=207.

[140] Graff, *The Threat Matrix*, p. 574. For a description of known sting operations among the post-9/11 homegrown jihadist terrorism plots, see CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera, Appendix A.

[141] Quoted in Basil Katz, "New York Bomb Plot Four Ask Judge to Dismiss Charges," *Reuters*, March 24, 2011, http://www.reuters.com/article/2011/03/25/us-security-newyork-plot-idUSTRE72O0CC20110325.

terrorists to detonate the bomb. In actuality, the device was a dud assembled by his co-conspirators, who were FBI undercover operatives. Mohamud offered the target for the strike, provided components for assembly of the device, gave instructions for the operation, and mailed passport photographs for his getaway plan to FBI undercover operatives.[142] What specifically caused the FBI to begin its sting operation against Mohamud is unclear from publicly available sources. At some point, someone from the local Muslim community alerted the FBI to Mohamud, a 19-year-old Somali-born naturalized U.S. citizen. Media reports have suggested that a family member, perhaps Mohamud's father, relayed concerns about the young man to officials.[143]

In a number of recent FBI terrorism sting operations, defense attorneys have alleged that the FBI had entrapped defendants.[144] Ten defendants charged with terrorism-related crimes have formally argued the entrapment defense in six trials since 9/11.[145] However, since 9/11 this defense has been unsuccessful in federal courts.[146] FBI Director Mueller and Attorney General Holder have described the use of sting operations as "essential" to terrorism prevention.[147] Mueller has emphasized that the FBI is careful in its undercover investigative work, arguing that the agency performs "substantial oversight" of the techniques used in these cases.[148]

In at least some investigations, FBI undercover employees test suspects to ascertain the depth of their intent to do harm. For example, the FBI evaluated Mohamud's resolve on a number of occasions. Two stand out. Mohamud's first meeting with an undercover FBI operative entailed a discussion in which the would-be violent jihadist was told that he could help "the cause" in "a

---

[142] U.S. Department of Justice, "Oregon Resident Arrested in Plot to Bomb Christmas Tree Lighting Ceremony in Portland," press release, November 27, 2010, http://portland.fbi.gov/dojpressrel/pressrel10/pd112610.htm.

[143] Caryn Brooks, "Portland's Bomb Plot: Who Is Mohamed Mohamud?" November 28, 2010, *TIME Magazine,* http://www.time.com/time/nation/article/0,8599,2033372,00.html.

[144] In criminal law, a person is "entrapped" when he is induced or persuaded by law enforcement officers or their agents to commit a crime that he had no previous intent to commit. A defendant who is subject to entrapment may not be convicted as a matter of public policy. However, there is no entrapment where a person is ready and willing to break the law and the government agents merely provide what appears to be a favorable opportunity for the person to commit the crime. Merely providing an opportunity to commit a crime is not entrapment. In order to find entrapment, there must be persuasion to commit a crime by the entrapping party. Entrapment is an affirmative defense in which the defendant has the burden of proof. It excuses a criminal defendant from liability for crimes proved to have been induced by certain governmental persuasion or deceit. To claim inducement, a defendant must demonstrate that the government conduct created a situation in which an otherwise law-abiding citizen would commit an offense. The defendant must show that he or she was unduly persuaded, threatened, coerced, harassed, or offered pleas based on sympathy or friendship by police. See *Legal Definitions and Legal Terms Dictionary*, U.S. Legal Forms, Inc., http://definitions.uslegal.com/e/entrapment/. See also William Yardley, "Entrapment is Argued in Defense of Suspect," *New York Times,* November 29, 2010, http://www.nytimes.com/2010/11/30/us/30mohamud.html; Chris Herring, "Bomb Case Bail Hearing," *The Wall Street Journal,* June 22, 2010, http://online.wsj.com/article/SB10001424052748704256304575321131297175098.html?mod=WSJ_hpp_sections_newyork; A.G. Sulzberger, "Defense Cites Entrapment in Terror Case," *New York Times,* March 17, 2010, http://www.nytimes.com/2010/03/18/nyregion/18newburgh.html; Carol J. Williams, "A Case of Terror or Entrapment," *Los Angeles Times,* November 30, 2007, http://articles.latimes.com/2007/nov/30/nation/na-liberty30; Michael Wilson, "Jury Convicts 2 Albany Men in Missile Sting," *New York Times,* October 11, 2006, http://www.nytimes.com/2006/10/11/nyregion/11plot.html.

[145] The Center on Law and Security, New York University School of Law, *TTRC Update: Informant Cases and the Entrapment Defense,* March 2011. (Hereafter: Center on Law and Security, March 2011.)

[146] Nardine Saad, "FBI Director Robert S. Mueller III in O.C. Denies Sting Operations Aimed at Terrorists Are Entrapment," *Los Angeles Times*, http://latimesblogs.latimes.com/lanow/2011/01/fbi-director-robert-s-mueller-iii-in-oc-denies-sting-operations-aimed-at-terrorists-are-entrapment.html. (Hereafter: Saad, "FBI Director.")

[147] Ibid; Malia Wollan and Charlie Savage, "Holder Calls Terrorism Sting Operations 'Essential,'" *New York Times,* December 11, 2010, http://www.nytimes.com/2010/12/12/us/politics/12holder-1.html.

[148] Saad, "FBI Director."

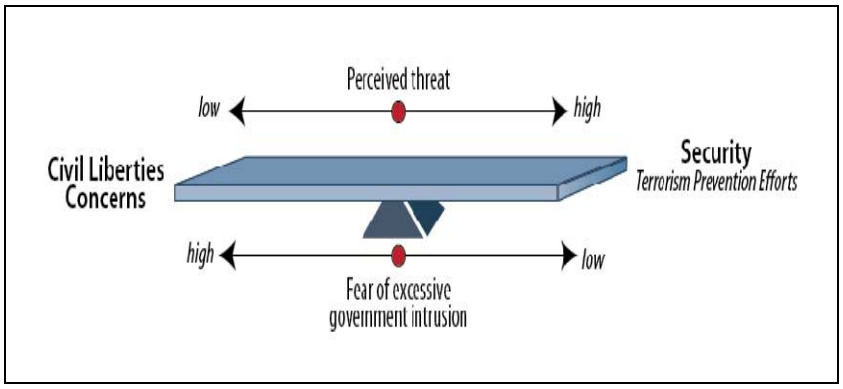
number of ways … ranging from simply praying five times a day to becoming a martyr." The young man responded, saying that he wanted to become "operational" and needed help in staging an attack. When Mohamud suggested the Christmas tree lighting ceremony as his intended target in a following meeting, an FBI undercover employee noted that children attend such events. Mohamud responded by saying that he wanted a large crowd "that will … be attacked in their own element with their families celebrating the holidays."[149]

Balancing Civil Liberties against Terrorism Prevention

As discussed, the FBI's DIOG articulates a *need* to proactively gather intelligence in counterterrorism investigations and establishes the assessment as a technique to do so. Balancing civil liberties against the need for preventative policing to combat terrorism is a key policy challenge. The notion of balancing civil liberties against security requirements is not new. In 1976, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly referred to as the Church Committee after its chair, Senator Frank Church) noted as much in its investigation of domestic intelligence abuses:

> A tension between order and liberty is inevitable in any society. A Government must protect its citizens from those bent on engaging in violence and criminal behavior, or in espionage and other hostile foreign intelligence activity.… Intelligence work has, at times, successfully prevented dangerous and abhorrent acts, such as bombings and foreign spying, and aided in the prosecution of those responsible for such acts.

Figure 1. Balancing Civil Liberties Concerns and Security



Source: CRS.

But intelligence activity in the past decades has, all too often, exceeded the restraints on the exercise of governmental power that are imposed by our country's Constitution, laws, and traditions.[150]

[149] Ibid; United States v. Mohamed Osman Mohamud, Criminal Complaint, U.S. District Court for the District of Oregon, November 26, 2010, p. 2, http://media.oregonlive.com/portland_impact/other/USAFFIDAVIT.pdf.

[150] Church Committee, *Book II,* p. 2.

Figure 1 suggests how competing elements influence the balance between civil liberties and security—largely defined today in terms of terrorism prevention efforts. As an historical example, the FBI had developed intrusive domestic intelligence collection measures and counter-radical operations stretching from the late 1930s through the 1960s. Of course, the focus of the FBI's efforts in this period was not counterterrorism. These decades featured domestic security concerns during World War II and fears of espionage and communist infiltration of American institutions during the Cold War. The FBI worked to prevent this activity. For much of this period, a national consensus suggested that serious threats were posed by foreign agents, revolutionaries, or outside agitators operating in the United States. Within this context, the FBI had broad authority for investigation of and intelligence collection regarding domestic subversive activity from Presidents Harry S. Truman and Dwight D. Eisenhower and Attorney General Robert F. Kennedy.[151] The agency developed a number of programs to combat what it saw as internal threats.

During this period, the FBI engaged in what can be described as preventive, covert, intelligence-based efforts to target and contain people, groups, or movements suspected by the agency to be '"rabble rousers,' 'agitators,' 'key activists,' or 'key black extremists.'"[152] A hallmark was the agency's Counterintelligence Program (COINTELPRO), which lasted from 1956 to 1971. Subjects investigated by the FBI under its domestic intelligence programs did not have to be suspected of criminal activity. Instead of bringing criminal cases to court, the Bureau acted outside of legal processes and relied on illegal means to curb constitutionally protected activity it deemed threatening to national security.[153]

COINTELPRO

Prior to 1976, national security investigations at the FBI followed no specific guidelines established by either DOJ or Congress. Without oversight, the agency developed a covert Counterintelligence Program (COINTELPRO) to target the Communist Party U.S.A.[1] During its lifespan from 1956 to 1971, the program involved aggressive and illegal tactics to harass, disrupt, discredit, and collect intelligence on the party and its members. COINTELPRO's purpose was to protect national security, prevent violence, and maintain the social and political order in the United States.[1] It was not designed to build traditional cases to be brought to trial. The FBI expanded COINTELPRO to target groups and movements such as the Socialist Workers Party, the Ku Klux Klan, the New Left, and the Black Panther Party.[1] The program was developed partly because the FBI was frustrated with Supreme Court limits on overt investigations of dissident groups.[1]

With COINTELPRO, the FBI "took the law into its own hands"[1] and authorized questionable methods including "use of subterfuge, plant[ing] agents provocateurs, [and] leak[ing] derogatory information to the press."[1] Among specific tactics, the FBI mailed anonymous letters to break up marriages, contacted employers to get people fired from their jobs, and falsely declaimed individuals as government informants to discredit them within their own organizations.[1] The agency even targeted some nonviolent organizations, such as the Southern Christian Leadership Conference, because it "believed they represented a 'potential for violence.'"[1] As the FBI itself acknowledges, some COINTELPRO methods were excessive and "went too far for the American people."[1]

The public first learned of the program after a 1971 burglary at an FBI office in Media, PA. Individuals tied to the incident leaked information on COINTELPRO to the press and Congress. In response, the FBI terminated the program.[1]

By the 1970s, as Cold War fears ebbed, the balance between civil liberties and prevention tipped in the other direction—favoring concerns over civil liberties. This is highlighted by the development of the original set of Attorney General guidelines. Issued in 1976 and known as the *Domestic Security Investigation Guidelines*, these responded to FBI abuses embodied in programs

[151] Church Committee, *Book II*, p. 39.

[152] Church Committee, *Book II*, pp. 40, 69.

[153] Ibid; Church Committee, *Book III,* pp. 211-212.

such as COINTELPRO. These first guidelines were intended to prevent the FBI's monitoring of groups that had unpopular or controversial public views and greatly circumscribed the agency's domestic intelligence gathering capabilities and investigations related to national security-related issues.[154]

Since the 1976 guidelines, and especially after 9/11, the balance has shifted in favor of security and terrorism prevention efforts. As suggested, the Mukasey Guidelines and FBI DIOG offer more investigative flexibility to proactively counter terrorist actors. Critics have stated that subsequent guidelines have excessively loosened the constraints on FBI intelligence collection and investigation.[155] In essence, these critics suggest that concerns over terrorism and security have outweighed fears of systemic abuse by investigators.

Philadelphia Inquirer reporter and author Stephan Salisbury describes current efforts at striking this balance as the "bind" the FBI finds itself in. "On one hand it is being charged by the Justice Department to go out and stop this stuff [terrorism] before it happens. But on the other, it is getting criticized for the techniques it is using to do that."[156] The Mukasey Guidelines and FBI DIOG address the same competing forces, and, as mentioned, their implementation has spurred concerns among civil liberties groups.

Considerations for Congress

Since 9/11, the FBI has been given substantially greater resources to enhance its counterterrorism activities—particularly its intelligence operations.[157] The Bureau over the last decade has also introduced a series of reforms intended to transform it from a largely reactive law enforcement agency focused on criminal investigations into a more proactive, agile, flexible, and intelligence-driven organization.

In its oversight role, Congress may wish to examine the extent to which intelligence has been integrated into FBI operations to support its counterterrorism mission and the progress the Bureau has made on its intelligence reform initiatives. Congress may also wish to explore the extent to which the FBI has enhanced its collaboration with the Department of Homeland Security, other federal partners, and state and local law enforcement elements. This is not just an issue of information sharing, but of how the Bureau has institutionalized its collaboration in order to tackle complex threats. Finally, Congress might ask how the FBI uses strategic intelligence to develop a true understanding of security threats and how they are evolving. In other words, has the Bureau developed effective predictive capacity?

FBI intelligence reforms since 9/11 have met with a mixed response. Among its intelligence initiatives since 9/11, the FBI has increased its intelligence focus by creating a Directorate of Intelligence and hiring thousands of new and better-qualified analysts. Another innovation was

[154] Berman, *Domestic Intelligence,* p. 11.

[155] Berman, *Domestic Intelligence,* p. 13.

[156] Stephan Salisbury, "Leather Glove," audio interview, *tomdispatch.com*, July 5, 2010. http://tomdispatch.blogspot.com/2010/07/leather-glove.html. (Hereafter: Salisbury, "Leather Glove.")

[157] The FY2012 budget request for the FBI proposes $131.5 million for new or expanded initiatives and 181 new positions, including 81 special agents, three intelligence analysts, and 97 professional staff. See Mueller Testimony, April 6, 2011.

the establishment of Field Intelligence Groups (FIG) that are embedded into each of the FBI's 56 field offices. The FBI says that the FIGs are responsible for coordinating, managing, and executing all the functions of the intelligence cycle. In April 2011, Director Mueller testified that "the FBI recently restructured its FIGs, where each group now has clearly defined requirements for intelligence collection, use, and production. With this new structure, each office can better identify, assess, and attack emerging threats."[158]

Yet, as the Senate Homeland Security and Governmental Affairs Committee (HSGAC) investigation into the Fort Hood shootings highlighted, questions remain about the extent to which intelligence has been effectively integrated into FBI investigative operations. According to the Senate HSGAC's report, *A Ticking Time Bomb:*

> In the Hasan case, the FBI did not effectively utilize intelligence analysts who could have provided a different perspective given the evidence that it had. The FBI 's inquiry focused narrowly on whether Hasan was engaged in terrorist activity - as opposed to whether he was radicalizing to violent Islamist extremism and whether this radicalization might pose counterintelligence or other threats (e.g., Hasan might spy for the Taliban if he was deployed to Afghanistan). This critical mistake may have been avoided if intelligence analysts were appropriately engaged in the inquiry.[159]

Congress may wish to examine the extent to which analysts at the FIGs have access to case information about specific Joint Terrorism Task Force (JTTF) investigations and the opportunity to provide relevant intelligence to help steer those investigations. The FBI Intelligence Analysts Association has stated that analysts at the FBI continue to be relegated to "support" roles[160] (i.e., they react to direction from special agents rather than being full partners in an intelligence-driven investigative operation). They argue that intelligence analysts should have professional parity with special agents to rapidly reform the FBI's institutional culture.

Congress may also wish to explore the extent to which intelligence analysts outside the FIGs, such as those within the Directorate of Intelligence at Headquarters, also have access to case information about specific JTTF investigations and have the opportunity to provide relevant intelligence for those investigations. According to the Senate HSGAC report:

> In the Hasan case, two JTTFs (each located in a different field office) disputed the significance of Hasan's communications with the Suspected Terrorist and how vigorously he should be investigated. The JTTF that was less concerned about Hasan controlled the inquiry and ended it prematurely after an insufficient examination. Two key headquarters units - the Counterterrorism Division, the "National JTTF" (which was created specifically to be the hub among JTTFs), and the Directorate of Intelligence were not made aware of the dispute. This unresolved conflict raises concerns that, despite the more assertive role that FBI headquarters now plays, especially since 9/11 in what historically has been a decentralized organization, field offices still prize and protect their autonomy from headquarters. FBI headquarters also does not have a written plan that articulates the division of labor and hierarchy of command-and-control authorities among its headquarters units, field offices, and the JTTFs.[161]

[158] Mueller Testimony, April 6, 2011.

[159] *A Ticking Time Bomb,* p. 10.

[160] FBI Intelligence Analysts Association, *Intel Shift "Needs To" Happen,* February 26, 2010.

[161] *A Ticking Time Bomb*, p. 10.

Insight by Directorate of Intelligence (DI) analysts into JTTF cases would enable the DI to provide national intelligence community-level support to help guide those cases. It would also facilitate DI analysis of the overall domestic terrorism threat so it can provide strategic context to the FBI leadership and other policy makers.

Finally, the FBI has greatly increased its production of intelligence products. As noted earlier, in 2010 the Bureau produced over 25,000 intelligence reports on counterintelligence, counterterrorism, and criminal topics as well as information related to cyber issues and weapons of mass destruction.[162] It may be of oversight interest to Congress to examine the value of these reports, their accessibility within the intelligence and law enforcement communities, and the views of various consumers about them.

Author Contact Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

Acknowledgments

Mark A. Randol, former CRS Specialist in Domestic Intelligence and Counter-Terrorism was originally a co-author of this report.

[162] *FBI Information,* p. 22.