Intelligence, Police, and Counterterrorism: Assessing Post-9/11 Initiatives

Peter Chalk and William Rosenau

30 October 2003

I. Introduction

The 11 September 2001 attacks on the World Trade Center and the Pentagon prompted a wide-ranging debate over the domestic intelligence, the relationship between intelligence and law enforcement, and what was required to defend the American homeland against terrorist threats. During the course of this debate, two important inter-related questions emerged. The first concerned collection: Were police and intelligence agencies collecting sufficient information on threats to the homeland, and if not, could more be done without jeopardizing civil liberties? The second question centered on analysis. Specifically, why did the relevant agencies seem unable to "connect the dots" and piece together information necessary to prevent terrorist attacks?

In the two years following the September 2001 terrorist strikes, governmental bodies, journalists, and policy analysts have advocated a variety of measures intended to improve domestic counterterrorism intelligence. Most of these critics focused on shortfalls within the Federal Bureau of Investigation (FBI), the law enforcement and intelligence agency with the lead responsibility for identifying and defeating terrorist threats to the US homeland. Recommendations for reform included the establishment of a new domestic security service along the lines of Britain's MI5. Intelligence would be separated from law enforcement, with the former given to the new agency, and the latter responsibility left with a rump FBI. Such an

organization, according to its supporters, would focus on prevention, rather than simply investigating terrorist acts once they occurred.[1] Critics of the concept charged that it would add needless complexity to the system, slow down rather than promote information flows among agencies, and threaten civil liberties.[2]

Ultimately, the Bush administration rejected calls for the creation of an "American MI5," choosing instead to press for reforms within the FBI and the creation of new bureaucratic arrangements within other parts of the federal government. The FBI's leadership has outlined a comprehensive program of internal changes that are intended to make the prevention of terrorism the bureau's paramount mission. In addition, new information collection and assessment structures have been created, including, notably, a dedicated Information Analysis and Infrastructure Protection Directorate (IAIP) within the Department of Homeland Security (DHS) and a separate Terrorist Threat Integration Center (TTIC).

As dramatic as some of these changes appear to be, it is unclear whether they will be able to address or overcome the main deficiencies that have been identified in U.S. domestic counterterrorism intelligence, including problems involving inter- and intra-agency communication, data dissemination, threat assessments, and structural coordination. The purpose of this paper is twofold. First, it will describe in general terms the changes underway at the federal level. Second, it will assess those changes and, where appropriate, suggest ways of improving the reform process. To add additional texture to the discussion, this paper includes references to the experiences of other democratic countries (specifically, Britain, Canada, and Australia), as well as reactions to these initiatives from

US federal and non-federal security officials. It should be noted, however, that this assessment is necessarily preliminary in nature. The changes underway in the federal system have been in place for a relatively short time, and are thus too new to judge in a comprehensive fashion.

This paper is divided into four sections. Following this introduction, part II outlines FBI counterterrorism structures as they existed before 9/11. Part III considers the bureaucratic changes since 9/11 that are intended to improve intelligence collection and analysis involving threats to the US homeland. Finally, part IV offers a set of recommendations for building on the reform initiatives now underway.

II. FBI Counterterrorism Structures before 9/11

Despite a heavy emphasis on law enforcement, the FBI built up a broad domestic intelligence and counter-intelligence program during the Cold War, the basic thrust of which was directed at stemming communist subversion within the United States. Largely because this information-gathering agenda was institutionalized in the absence of any system of congressional legislative authorization or oversight, its direction took on an increasingly explicit political character that was applied to a widening range of ordinary American citizens involved in such (legal) domestic pursuits as civil rights marches and anti-war protests.[3]

In reaction to these abuses, significant limits were placed on the bureau's information gathering techniques, particularly as they pertained to the monitoring of religious institutions, political organizations and individual suspects who had yet to commit a crime (the so-called "Levi guidelines"). At the same time, considerable pressure was placed on the FBI to return to a narrower definition of its traditional law enforcement mission, which combined with the aforementioned surveillance restrictions, resulted in a considerably paired down domestic intelligence structure that was almost exclusively geared towards data that related to the commission of specific crimes undertaken by one or more individuals.[4]

Growing dangers from domestic and international terrorism forced the FBI to devote more of its resources to counterterrorism during the 1980s and, especially, the 1990s. In 1982, counter-terrorism was designated a fourth national priority for the bureau and in 1986, the Justice Department sanctioned its agents with the power to arrest terrorists, drug traffickers and other fugitives abroad

without the consent of the foreign country in which they resided. In 1999, following the East Africa embassy bombings, the bureau established a Counterterrorism Division (CTD) to focus FBI resources on the terrorist threat.[5]

Despite these moves, the FBI never developed a truly coordinated, systematic domestic counterterrorism intelligence capacity. This was due in part to the bureau's own stress on traditional, case-based criminal investigations, and in part to the on-going salience of a national political context that was anxious to ensure the intelligence abuses of the past would not be repeated. Over time, special agents became reluctant to associate with any sort of "undesirables," even when such sources could provide important information on terrorism.[6] As a result of these factors, human intelligence (HUMINT) was a relatively under-utilized tool within the FBI. "Agents [did not] like to go into mosques," two journalists concluded recently, adding that the "so-called right of sanctuary was drummed into young FBI agents during their training at Quantico: 'You don't chase a thief into a cathedral.'"[7]

Bureaucratic arrangements also contributed to serious shortfalls. Highly autonomous field offices (FOs) lacked the means and often the will to communicate beyond their specific territorial borders and jurisdictions.[8] Because of these various organizational traits and concerns, the essence of the FBI's pre-9/11 information gathering remained ad-hoc, decentralized, reactive and case-based in nature. Responsibility for taking the lead in terrorism cases lay with local FOs rather than the central headquarters and frequently the dissemination of important information was precluded by the lack of modern computer hardware and secure emailing technologies. Extant legal prohibitions prevented the initiation of proactive domestic surveillance,

effectively ruling out the possibility of mounting operations to stem potential or probable violations of the law.

Finally, and perhaps most significantly, only important investigative data that had specific foreign value or equity (for example, espionage) tended to be shared with the wider intelligence community, with most other types of intelligence – even if it related to counterterrorism - typically closely guarded for the sake of protecting the integrity of pursuant criminal cases.

Many of these deficiencies have been identified in the findings of blue ribbon inquiries and task forces instituted in the wake of September 11. The Markle Foundation's Task Force on Protecting America's Freedom in the Information Age specifically alludes to the law enforcement "mentality" of the FBI as a major factor mitigating the development of an effective domestic counterterrorism capability.[9] Equally, recommendations of the Joint House-Senate Inquiry into the Terrorist Attacks of September 11 reflect a concern with the lack of organization and structure in the FBI's overall domestic counterterrorism function, particularly the agency's failure to clearly articulate and enforce national counterterrorism priorities as well as its general inability to provide for coherent, all-source terrorism information fusion.[10]

In a similar vein, the Fourth Annual Report of the Gilmore Commission notes a dearth of effective coordination between the FBI, the Central Intelligence Agency (CIA) and other members of intelligence community as well as serious gaps in the bureau's systematic analysis of terrorist threats in the United States.[11] Finally the General Accounting Office (GAO) singles out communications as a "long standing problem for the FBI" and one that has

significantly hampered the sharing of time-sensitive information both within the bureau and across other intelligence agencies.[12]

A call to establish a new domestic counterintelligence service was the most dramatic recommendation to emerge from these public and private inquiries. The experiences of other democratic countries suggested that other models for combating terrorism—if not directly applicable to the United States—are worth considering.[13] Unlike the FBI, the British Security Service ("MI5"), the Australian Security Intelligence Organization (ASIO), and the Canadian Security Intelligence Organization (CSIS) have no powers of arrest. Rather, working closely with local police—which serve as a critical source of information--these organizations monitor, surveil, and analyze groups that are deemed threatening to national security. With a heavy reliance on HUMINT collection, these services work to disrupt terrorist attacks; indeed, they embody a "culture of prevention," a concept embraced by the FBI only recently.

How effective these foreign services are in preventing terrorism is open to debate. Their supporters highlight the specialized skills (including language proficiency), their ability to monitor targets for years and develop a deep understanding of terrorist motivation and behavior, and their close relationships with law enforcement agencies. Critics, on the other hand, charge that the reputations of these services is overblown; that the services by their very nature pose a threat to civil liberties; and that the services and the police, far from working together, are frequently at odds. Given the secrecy and sensitivity that surrounds counterterrorism activities, it is difficult to assess their contribution.[14] That said, it seems clear that a security organization that operates outside the confines

and demands of case-based law enforcement develop capabilities—including foreign language, agent handling, and assessment skills—that are critical parts of an effective counterterrorism intelligence campaign.

III. Federal Counterterrorism Intelligence Initiatives Since 9/11

In the wake of the 2001 attacks in New York and Washington, major emphasis has been devoted to overhauling U.S. structures of domestic intelligence gathering and assessment. Several important reforms have been instituted, both specifically within the FBI and more generally in the context of upgrading homeland security.

FBI initiatives

Significant changes have taken place at the FBI in the months since the September 11 attacks, structurally, functionally, and operationally. Most fundamentally, there has been a major overhaul and expansion of the FBI's CTD, which will now take the lead in all terrorism-related cases from FOs. Integral to this re-organization has been the creation of an Executive Assistant Director for Intelligence responsible "first and foremost for counter-terrorism and the transfer of 150 counterterrorism personnel to the bureau's central headquarters in Washington DC. [15] The idea is to build "bench strength" in a single location rather than having expertise dispersed (and thereby diluted) across multiple jurisdictional sites.[16]

To give added force to the CTD, specialized "flying squads" are to be set up to coordinate national counter-terrorism investigations and augment local field capabilities. These highly deployable units are intended to provide a "surge capacity" for quickly responding to and resolving unfolding contingencies, particularly in areas where there is either a residual or absent FBI presence.[17]

A new National Joint Terrorism Task Force (NJTTF) has also been established, which will be equipped with a 24-7 Counter-Terrorism Watch List (TWL) and two sections on Document Exploitation and Communications Analysis Center. The NJTTF will complement and coordinate the existing pool of 66 (up from 35 before September 11) city-level Joint Terrorism Task Forces (JTTFs) and six Regional Terrorism Task Forces (RTTFs)[18] already in place across the country to facilitate the efficient and effective flow of information between Federal, state and local jurisdictions and intelligence agencies.[19]

In addition to increasing the core strength and management of the CTD, a major effort is underway to redirect the FBI's general employee base to dedicated counter-terrorism duties. Specifically, 518 agents are to be shifted to this area - 400 from narcotics and 118 each from white-collar crime and violent crime. Of these personnel, 480 will be permanently re-assigned, which represents roughly 30 percent of the former's and between two and three percent of the latter's pre-9/11 staffing levels.[20]

Complementing the re-organization and re-focusing of the FBI's counterterrorism capabilities have been several analytical enhancements, particularly in the area of strategic intelligence.[21] In December 2001, an Office of Intelligence was created, which will support both counterterrorism and more generic counter-intelligence (CI) and will focus on improving the bureau's ability to collect, consolidate, assess and disseminate information on vital national security matters. The Office will also oversee the development of a College of Analytical Studies (CAS), which will train FBI recruits in the latest intelligence assessment and forecasting procedures and which is designed to lay the foundation for a dedicated analyst career track

that would be of interest to those not normally attracted to a future in pure law enforcement.[22]

To ensure that this new complement of analysts has adequate intelligence and communication tools at their disposal, substantial investments are being made to address the shortcomings in FBI information technology (IT). A US$379 million multi-phased process (known as Trilogy) intended to upgrade the Bureau's capacity to collect, store, search, retrieve, assess and disseminate data is presently underway, and by January 2004 will provide all bureau field sites with improved network communications, a common and current set of office automation tools and user-friendly, re-engineered web-site applications.[23] A three-step IT infrastructure enhancement strategy has also been planned. Ultimately this will allow classified data to be shared internally among FBI analysts and disseminated externally to the wider IC.[24]

In addition to organizational and structural modifications, the bureau's leadership has begun a series of functional changes designed to make the FBI more proactive. The thrust of these reforms have been aimed at relaxing old rules restricting the monitoring of religious institutions, political organizations and individual suspects without first establishing probable cause they were involved in criminal activity. In addition former prohibitions preventing special agents from attending public gatherings and/or pursuing terrorist leads in generic databases and on the Internet have largely been scrapped.[25] Clearly the bureau's expectation is that its special agents and analysts assigned to counterterrorism will adopt some of the positive features frequently associated with foreign services such as MI5, ASIO, and the CSIS—specifically, the use HUMINT and the

emphasis on developing a comprehensive understanding of the threat.

Reforms Instituted in the Context of U.S. Domestic Homeland Security

The Department of Homeland Security (DHS)

The DHS – established in the wake of 9/11 to rationalize and coordinate the numerous agencies and entities concerned with U.S. domestic counter-terrorism[26] - includes an Information Analysis and Infrastructure Protection (IAIP) Directorate dedicated to strategic analysis. The organization's roles, missions, and functions are still being determined, although it is possible to describe its general contours. The office will collate and assess data from multiple sources - including the FBI, CIA, National Security Agency (NSA), Drug Enforcement Administration (DEA), Energy Department, Customs Service and Transportation Department - and is intended to act as a central fusion point for all information relevant to homeland security and related critical infrastructure protection (CIP) threat contingencies. Although the IAIP has no specific collection powers of its own, it is mandated to receive "raw" intelligence from both the FBI and CIA and over time may be accorded the right to "task" each with directed data gathering functions that reflect its own mission priorities and agendas.[27]

In the judgment of one senior US intelligence official, the IAIP should (ideally) serve as transmission belt between the intelligence community, which produces threat information, and "non-federal" officials responsible for defending key infrastructure targets.[28] In the past, federal, state, and local agencies rarely produced threat assessments, focusing instead on the easier task of

identifying vulnerabilities. Under these new arrangements, threat assessments may become more regular, with IAIP translating threat information provided by the intelligence community into a form useful to non-federal public-safety officials.[29]

The Terrorist Threat Integration Center

In May 2003, an independent terrorist threat integration center commenced operations as part of the on-going effort to minimize seams in the analysis of counterterrorism intelligence collected overseas and within the United States. TTIC will eventually co-locate the FBI's CTD and the CIA's Counter-Terrorism Center (CTC)[30] within a single facility that will also incorporate explicit representation from the Attorney General and the Secretaries of Homeland Security, Defense and State.[31] Under TTIC's terms of reference, the center will

- Conduct threat analysis and inform overall collection strategies - though in common with the ID at the DHS, TTIC will have no information gathering powers of its own;

- Create a structure to institutionalize the sharing of all terrorist intelligence across agency lines in order to generate the most detailed and informed threat picture possible;

- Provide on-going and comprehensive assessments to the national leadership;

- Oversee the development a national counterterrorism tasking and requirements system;

- Maintain an up-to-date database of known and suspected terrorists and ensure that this is made available to appropriate official at all levels of government.[32]

As noted above, the DHS will have explicit representation in the TTIC. The IAIP will receive and analyze terrorism-related information, using this data to: (1) map potential threats against existing vulnerability assessments; (2) take and recommend responses to identified challenges contingencies; and (3) set national priorities for CIP. The directorate will also act as the main intelligence conduit for the Federal government, ensuring that threat assessments generated by TTIC are disseminated quickly to the public, private industry and state and local government and law enforcement officials.[33]

IV. Observations and Recommendations

A. Observations

The changes instituted in the make-up of the American internal intelligence structure represent the most far-reaching process of reform in over half a century. In many ways, the modifications will equip the country with a more robust, comprehensive and rationalized structure for the collection, analysis and dissemination of counter-terrorism information.

First and most importantly, moves have been made to overhaul the intelligence function of the FBI, which remains the principal body charged with assessing and responding to threat contingencies in the United States. Principal elements of this re-alignment effort that are noteworthy include:

- Investments in communications and information management technology;
- The emphasis on developing rigorous, discretely focused analytical capabilities;
- Moves to establish a cadre of specifically assigned, professional counterterrorism specialists;
- Increased coordination of dispersed field office operations within the context of a singularly developed (and enforced) national counterterrorism strategy.

Second, measures have been taken to fuse and integrate the collection, assessment and dissemination of domestic counterterrorism intelligence across agency jurisdictional boundaries. Both the DHS' IAIP and TTIC represent important developments in this regard and will, for the first time,

provide organizational settings in which regular and comprehensive threat assessments can be generated and refined. This will greatly avail the policymaking process, particularly in terms of delineating national priorities and, thereby, helping to guide the strategic allocation of scarce resources.

This being said, several facets of the reform process either remain questionable or raise additional issues of concern. In no particular order of significance, these variously relate to: (1) the efficacy of changes enacted within the FBI; (2) the development of viable structures of accountability and oversight to balance more intrusive domestic information gathering; (3) the incorporation of local law enforcement in Federal counter-terrorist responses; and (4) the coordination of national intelligence structures.

Assessing Changes at the FBI

Although sweeping reforms have been promised and/or instituted at the FBI, it is not apparent how quickly or readily the agency will be able to switch from its traditional law enforcement focus. Certainly data on FBI criminal enforcement in the months since 9/11 does not suggest a major shift has occurred in the agency's focus of attention, the bulk of which continues to be dominated by drug violations, bank robberies and credit card fraud.[34]

The re-alignment of FBI staff also does not appear to have dramatically altered the overall deployment of the bureau's resources. Internal statistics indicate that by the beginning of 2002 the number of intelligence officers employed at the agency had actually declined by five percent. More pointedly, employees devoted to the counterterrorism field currently constitute roughly twenty percent of all bureau resources, which only slightly exceeds

the proportion that existed at the time of the September 11 attacks.[35]

The Development of Viable Structures of Accountability and Oversight

The U.S. Attorney General, John Ashcroft, has repeatedly assured that all post-9/11 counterterrorism intelligence initiatives have been carefully calibrated in full accordance with Constitutional safeguards and provisions. However, he has given no indication as to precisely how the institution of the new architecture is to be implemented, monitored or reviewed. No specific system of legislative and/or internal auditory accountability has yet been enunciated for TTIC and while the DHS will have several existing committees in the House and Senate monitoring its activities, Congress is not currently organized to oversee such a polycentric body in an effective manner.[36]

Significant difficulties are also extant with data protection. Presumably the dissemination of intelligence coordinated under the auspices of TTIC and the IAIP will be subject to the constraints of the 1974 U.S. Privacy Act, which aims to prevent the unwarranted disclosure of an individual's personal information.[37] However, this piece of legislation contains so many loopholes and exceptions that its enforcement mechanisms essentially amount to no more than paper shell protection.[38] Two in particular would allow for the largely unrestricted dissemination of, and access to private data within a counterterrorism setting. First, essentially all information obtained for specific national security and/or legitimate (however defined) law enforcement purposes is exempted from the Act's provisions. Second, the insertion of a "routine use" clause makes it possible for Federal agencies to obtain and disclose intelligence so long

as this is compatible with the purposes for which it was originally collected. Such a broad-ranging requirement does little to constrain the scope of counter-terrorism surveillance or, indeed, the operational mandates of existing and planned entities such as the FBI, CIA and TTIC.[39]

The loosening of investigative restrictions at the FBI is just as problematic. The bureau's expanded powers of covert information collection and monitoring will be governed by the strictures of the Foreign Intelligence Surveillance Act (FISA). Traditionally this legislative sanction required the government to demonstrate that the *sole* purpose of secret surveillance (where no prior crime had been committed) was to collect foreign intelligence. However, the USA PATRIOT Act modified this language to allow FISA orders to be issued in instances where a *significant* purpose of the surveillance is to obtain foreign intelligence.[40] Critics have challenged the constitutionality of this change, arguing that combined with the greater latitude afforded to the FBI, the government has effectively accorded itself the right to not only monitor perfectly legal activity by Americans but also to collect evidence for criminal prosecutions while avoiding the strictures of the Fourth Amendment.[41]

The issue of ensuring for viable and effective systems of oversight and control is not purely academic. The experience of countries such as Australia, Canada and the UK has shown that if intelligence structures and initiatives are not perceived to be transparent or accountable they will suffer from a credibility gap and almost certainly fail to receive the level of public trust and support necessary for their long-term invocation.[42] These considerations are relevant to the United States, a country where there is

deep-seated opposition to extending the remit of the federal government to the private sphere and where memories of past FBI abuses have engendered a palpable fear of the so-called "Big Brother" syndrome.

Incorporating State and Local Law Enforcement

Australia, Canada and the UK all integrate local law enforcement in their national counterterrorism responses in recognition that it is often at this level that indications of impending attacks first occur or decisive breaks in on-going cases eventuate. Moreover, it is in multi-cultural cities such as London, Sydney, and Vancouver that transnational terrorists often seek to establish logistical and operational cells or where they direct the bulk of their propaganda and fund-raising activities.[43]

In this manner, local law enforcement represents a valuable resource that national authorities can usefully tap for counter-terrorism purposes. Despite these evident benefits, the make-up of Washington's post-9/11 domestic intelligence architecture continues to reflect a federal-centric orientation. While moves are being made to more closely integrate state and municipal entities into national counterterrorism efforts - through, for examples, conduits such as the DHS – sharing of information remains ad-hoc and inconsistent. TTIC, according to one Los Angeles police official,

> still sees terrorism as a foreign intelligence problem and misses the domestic element. Where TTIC fits is ambiguous—it doesn't seem designed to pull up information from the local level.[44]

Although cities like New York and Los Angeles have long enjoyed close working relationships with the FBI,[45] the

bureau traditionally has been reluctant to share useful and timely information with smaller municipalities, and the organization continues to express concerns about operational security and intelligence leaks at the local level.[46] Critics have also charged that JTTF system, while promoting some greater information sharing, is too "FBI-centric," and that the bureau is remains dismissive of terrorism-related information supplied by state and local law enforcement agencies.[47] Given the growing recognition that routine, street-level policing can play a major role in preventing terrorism, the FBI's apparent lack of interest in information generated by state and local police poses a significant hurdle to improving domestic counterterrorism.[48] Finally, the FBI's continuing failure to produce a comprehensive threat assessment, which state and local require to allocate resources more effectively, suggests that the bureau has not yet fully embraced the new counterterrorism mission or fully recognized the importance of supporting non-federal public safety officials.[49]

Coordinating the New Intelligence Structures

The lack of effective coordination has long been recognized as a critical weakness in the make-up of U.S. national intelligence apparatus.[50] Although structures such as IAIP and TTIC have made certain improvements in terms of centralizing the analysis and dissemination of information, two serious weaknesses remain.

First, because neither the IAIP or TTIC have information gathering powers of their own, they will necessarily be reliant on a third party for the provision of domestic security intelligence – namely the FBI. Although the bureau has representation in the two bodies, its collection assets are not presently "owned" by either entity. There is, in other words, no formalized arrangement

that sets out the protocols and procedures for sharing information between the three agencies. This is problematic, not least because it remains unclear exactly how willing the FBI will be to pass on raw data for independent assessment. If little dissemination ultimately takes place, both the IAIP and TTIC will become moribund, degenerating into superfluous entities that are useless to policymakers, immaterial to the wider intelligence community and, at the end of the day, of no practical value in terms of intelligence coordination and fusion.[51]

Second, the institution of new intelligence structures, and the reform of existing ones, appears to be progressing in the absence of any overall guiding design or national strategy. It is not apparent, for example, how the analytical enhancements proposed for the FBI will interrelate with the capabilities of either the IAIP or TTIC or, indeed, how the latter two's mandate for CIP and threat warning will correlate with the bureau's (and CIA's) own general counterterrorism mission statement. So long as these issues remain unresolved, there will be a continuing danger of bureaucratic overlap and "stove-piping" – both of which will be directly detrimental to the setting of rational, sustainable priorities in the critical area of domestic counter-terrorism intelligence.[52]

B. Recommendations

In light of the above evaluation, several recommendations can be made to advance the process of domestic intelligence reform in the United States. Federally, protocols should be drawn up to govern the sharing of intelligence and "law-enforcement sensitive" information among the FBI, CIA, IAIP and TTIC, and between

these entities and relevant non-federal organizations. These formalized procedures should take the form of executive orders and, if necessary, classified National Security Presidential Directives and set out common guidelines on the ends, ways and means of collecting, analyzing and disseminating terrorist-relevant information.

In addition, more attention needs to be devoted to building and consolidating public credibility and trust. To achieve this, it is vital that the extension of FBI powers and the creation of TTIC and IAIP be accompanied by a legitimizing campaign that is sensitive to public concerns over potential civil liberties infringements, particularly with respect to covert surveillance and information storage and dissemination. No less importantly, the invocation, use and continuance of all strategic and operational intelligence measures should be made subject to a rational and easily understood system of administrative accountability. At a minimum this should embrace (1) comprehensive internal agency checks; (2) unfettered external auditing; (3) regular legislative oversight by a limited number of dedicated standing congressional committees; and (4) the annual release of appropriately "scrubbed" reports that can be freely examined in (and used to inform) the House, Senate and general public realm.

At the local level, a concerted effort should be made to institute an expedited system of clearances for carefully vetted and trusted police chiefs who could then act as intermediaries between the federal and state/local officials. Alternatively, federal officials could consider abandoning the costly, time-consuming, and cumbersome system of granting clearances and adopt a useful foreign model for intelligence sharing. In Britain, the Special Branch system serves as a bridge between the intelligence services and

local police by disseminating unclassified threat information in a form useful to law enforcement officers.

American policymakers might reconsider their belief that secret intelligence offers its customers a special, Gnostic wisdom, and encourage more dissemination of unclassified threat information. As the GAO recently concluded, "methods exist to declassify, redact, or otherwise adapt classified information so that it may be shared with state and local personnel without the need for granting additional security clearances."[53] For example, "we're used to writing in unclassified formats for foreign officials," notes one American intelligence official.[54]

Moreover, active consideration needs to be given to developing an all-channel communications network for the coordination of information across state law enforcement jurisdictions. Although many law enforcement agencies routinely share information with each other, the nature of the terrorist challenge requires even greater amounts of communication and coordination. A secure electronic medium that allows major city departments to directly interact with one another without first having to go through Washington would offer two important advantages. First, it would greatly speed the transmission of vital security information, which could then be used for either pre-emptive or response management purposes. Second, it would provide the necessary connectivity to integrate discrete "snapshots" of data into a single, coherently developed national picture.

Several state and metropolitan centers have already moved to establish integrated networks from the "bottom up," including Los Angeles, New York, Houston, Dallas and Philadelphia. These promising initiatives, which bring together a range of interested stakeholders from the police

to public health officials, should be supported and levered as building blocks from which to develop a more comprehensive system of national local law enforcement coordination.[55]

As the United moves to further consolidate its war on terrorism, it is vital that an effective machinery of domestic intelligence and counter-intelligence is put in place. Such as structure is vital in any open democratic society where vulnerabilities are vast but resources necessarily limited. Only by understanding the nature and scope of the terrorist threat through well-developed strategic assessments and evaluations will prudent decisions ultimately be made on how best to allocate preventative capabilities for future mitigation and security.

---

[1] See for example *The Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* [cited hereafter as the *Gilmore Commission Report*](Santa Monica, CA: RAND, 15 December 2002), pp. 41-44; and "Senator Edwards Proposes Homeland Intelligence Agency," accessed at http://www.cdt.org/security/usapatriot/030213edwards_pr.html.

2 See for example David Johnston, "F.B.I. Director Rejects Agency for Intelligence in the United States," *Washington Post*, 20 December 2002, p. A22; Larry M. Wortzel, "Americans Do Not Need a New Domestic Spy Agency to Improve Intelligence and Homeland Security," *Heritage Foundation Executive Memorandum* no. 848, 10 January 2003; and Ronald Kessler, "No to an American MI5," *Washington Post*, 5 January 2003, p. B07.

[3] *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (New York: Markle Foundation, October 2002), pp. 20, 89. For a discussion of past FBI abuses, including the notorious COINTELPRO program, see Sorrel Wildhorn, Brian Michael Jenkins, and Marvin M. Lavin, *Intelligence Constraints of the 1970s and Domestic Terrorism*, Vol. I, *Effects on the Incidence, Investigation, and*

Prosecution of Terrorist Activity, N-1901-DOJ (Santa Monica, CA: RAND Corp., December 1982), pp. 9-11.

[4] Ibid., p. 20.

[5] Ibid., pp. 85-86. See also Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, P.L. 107-56 (2001); and "FBI Names Assistant Director of Counterterrorism Division," FBI National Press Office Release, December 16, 1999.

[6] U.S. Congress, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence, *Report of Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, December 2002, p. 246.

[7] Evan Thomas and Daniel Klaidman, "The Battle Within," *Newsweek*, 15 September 2003, p. 40.

[8] Markle Foundation, *Protecting America's Freedom*, p. 20; David Walker, *FBI Reorganization: Initial Steps Encouraging But Broad Transformation Needed* (Washington D.C.: General Accounting Office, GAO-02-865T, June 21, 2002), p. 11; testimony of Robert Mueller before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, Joint Intelligence Committee Inquiry, United States Congress, Washington D.C., October 17, 2002; Gordon Corera, "US Reforms Overlook Threat from Foreign Intelligence," *Jane's Intelligence Review* (June 2003), p. 45; and "FBI: Al-Qaeda Seeks to Top Sept. 11," *USA Today*, February 05, 2003.

[9] Markle Foundation, *Protecting America's Freedom*, p. 21.

[10] See Recommendations of the Final Report of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001, United States Select Committee on Intelligence Press Releases, available on-line at http://intelligence.senate.gov/press.htm

[11] *Gilmore Commission Report*, Chapter V.

[12] Walker, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, 11.

[13] See for example "Recommendations of the Final Report of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001," United States Select Committee on Intelligence Press Releases, available on-line at http://intelligence.senate.gov/press.htm.

[14] For more on these services, see U.S. General Accounting Office [GAO], Combating Terrorism: How Five Foreign Countries are Organized to Combat Terrorism (Washington, DC: GAO, April 2000); Todd Masse, "Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States," Congressional Research Service, 19 May 2003; Jim Dempsey, "Domestic Intelligence Agencies: The Mixed Record of the UK's MI5," 27 January 2003, Center for Democracy and Technology, pp. 2-5, accessed at www.cdt.org; and Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies* (RAND, forthcoming 2004).

[15] The FBI intendeds to backfill these positions in the field through a major recruiting drive.

[16] Transferred staff would be expected and encouraged through incentives to remain in counter-terrorism work for an extended period of time both to enhance individual skill-levels and to deepen trust and familiarity in cooperative working relationships. This represents a notable

departure from the FBI's traditional procedure of regularly rotating agents through a variety of assignments.

[17] Walker, *FBI Reorganization: Initial Steps Encouraging but Transformation Needed*, 7-8; The White House, "Fact Sheet: Strengthening Intelligence to Better Protect America" White House press release, February 14, 2003, available on-line at http://www.whitehouse.gov/news/releases/2003/02/print/20030214-1.html.

[18] The RTTFs operate on an ad-hoc basis.

[19] Mueller, testimony before the Joint Intelligence Committee Inquiry; The White House, "Fact Sheet: Strengthening Intelligence to Better Protect America"; Markel Foundation, *Protecting America's Freedom in the Information Age*, p. 118; Robert Jordan, testimony on information sharing given before the US Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and Courts, Washington, D.C., April 17, 2002, available on-line at http://www.fbi.gov/congress/congress02/jordan0-41702.htm As part of this effort, the FBI has also instituted a pilot Joint Terrorism Task Force Information Sharing Initiative (JTTF ISI) involving the St. Louis, San Diego, Seattle, Portland, Norfolk and Baltimore field offices. This scheme is designed to integrate flexible search tools that will permit investigators and analysts to perform full text (as opposed to more narrow indices) searches of investigative files.

[20] Walker, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, 4-5; "Protecting the Nation: The FBI in War and Peace," TRAC: FBI-New Findings on FBI Criminal Enforcement, Syracuse University, April 2002, available on-line at: http://trac.syr.edu/tracfbi/findings/aboutFBI/keyFindings.html; "FBI Stung into Beefing Up Fight Against Terror," *The Financial Times*, 31 May, 2002.

[21] Shortcomings in the FBI's strategic intelligence capabilities were recognized as far back as 1998. Indeed even internal Bureau audits noted that the agency lacked sufficient quantities of high-level analysts, with most having little or no training in intelligence assessment procedures and most devoid of either academic or professional experience in the subject matter for which they were responsible. A May 2000 Justice Department report similarly found that the FBI lacked a viable information management system to correlate and integrate extrapolated field intelligence. For further details see GAO, *Campaign Financing Task Force: Problems and Disagreements Initially Hampered Justice's Investigation*, GAO/GGD-00-101BR (Washington D.C.: GAO, May 31, 2000).

[22] Mueller, testimony given before the Joint Intelligence Committee Inquiry; Walker, *FBI Re-Organization: Initial Steps Encouraging but Broad Transformation Needed*, 8.

[23] Mueller, testimony given before the Joint Intelligence Committee Inquiry; Rozen, "Information Sharing at the FBI," 120. See also McGee, "Mueller Jumps Critics by Building His Own Domestic Intelligence Program"; "How Outdated Filing Hampers FBI Ability to Fight Terrorism," *The Wall Street Journal*, July 09, 2002; "FBI Stung Into Beefing Up Fight Against Terror," *The Financial Times*, 31 May, 2002; and "Rewiring the FBI; The FBI's $379 Million Upgrade Won't Solve the Agency's Problems," *Wired*, October 2001, available o-line at http://www.wired.com/wired/archive/10.01/mustread.html

[24] Mueller, testimony given before the Joint Intelligence Committee Inquiry.

[25] Walker, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, 12; Gordon Corera, "Changes Needed in Information Sharing," *Jane's Intelligence Review* (August 2003): 4; "Government will Ease Limits on Domestic Spying by F.B.I" *The New York Times*, May 29,

2002; "Administration Begins to Rewrite Decades-Old Spying Restrictions," *The New York Times*, November 30, 2002. These reforms have been instituted within the broader context of the U.S. Terrorist Information Awareness (formerly Total Information Awareness/TIA) program, which has been developed by the Defense Advances Research Projects Agency and which entails in-depth searches of private electronic information storage systems to identify patterns of activity suggestive of terrorist activity.

[26] The DHS commenced operations in October 2002 under Presidential Executive Order 13228. The Department is run within the White House and is modeled on the National Security Council (NSC). It is headed by the Assistant to the President for Homeland Security (currently Tom Ridge) and combines the budgets and jurisdictions of eight Cabinet-level departments and agencies, including the Immigration and Naturalization Service, the Customs Service, the Department of Agriculture, the Coast Guard, the Federal Protective Service, the Transportation Security Administration, the Secret Service and the Federal Emergency Management Agency. The importance accorded to the new organization is reflected both by the fact that it has been placed within the Executive Office of the President and that the Director, Tom Ridge, has been assigned cabinet-level status. For further details see Peter Chalk and Rohan Gunaratna, *Jane's Terrorism and Counter-Terrorism* (London: Jane's Information Group, 2002), 130; "Re-organizing the Cabinet is a Complex Job," *USA Today*, June 07, 2002.

[27] Markle Foundation, *Protecting America's Freedom*, p. 71-72; Corera, "US Reforms Overlook Threat from Foreign Intelligence," 46; *Gilmore Commission Report*, p. 41; "Connect the Cops to Connect the Dots," *San Diego Tribune*, June 01, 2003;; "Administration Begins to Rewrite Decades-Old Spying Restrictions," *The New York Times*, November 30, 2002.

[28] Author's interview with senior intelligence official, Arlington, VA, 6 August 2003.

At the time of writing five divisions with a combined budget of $708 million had been planned, including a Critical Infrastructure Office; a Federal Computer Incident Response Center; a National Communications Systems Center; a National Infrastructure Protection Center; and a National Infrastructure Simulation and Analysis Center.

[29] "Re-organizing Cabinet is a Complex Job," *USA Today*, June 07, 2002.

[30] The CTC was created in 1986 to facilitate inter-agency cooperation in the collection of intelligence on international terrorist groups and state sponsors. Fifteen organizations are represented in the Center, including the CIA, FBI, Secret Service, Bureau of Alcohol and Tobacco and Firearms (ATF), the Immigration and Naturalization Service (INS), the National Security Agency (NSA), State Diplomatic Security (SDS), the Federal Aviation Administration (FAA), the Naval Criminal Investigative Service (CIS) and the Department of Energy (DoE). William Studeman, testimony given for the Omnibus Counterterrorism Act of 1995 before the House of Representatives Judiciary Committee, 06 April, 1995. For an analysis of the CTC and its role in homeland security see Stephen Marrin, "Homeland Security and the Analysis of Foreign Intelligence," background research report prepared for the Markle Foundation Task Force, Protecting America's Freedom in the Information Age.

[31] The White House, "Fact Sheet: Strengthening Intelligence to Better Protect America"; McGee, "Mueller Jumps FBI Critics by Building His Own Domestic Intelligence Program"; Pasquale D'Amuro, "Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center," statement given before the Senate Governmental Affairs Committee, U.S. Senate, Washington D.C. February 26, 2003; "Connecting the Cops to Connect the Dots."

[32] White House, "Fact Sheet: Strengthening Intelligence to Better Protect America."
[33] White House, "Fact Sheet: Strengthening Intelligence to Better Protect America."
[34] "Protecting the Nation: The FBI in War and Peace." During each of the last four years, for instance, drug violations, bank robberies and credit card fraud were the subject of more than one third of all FBI referrals for prosecution and over half of its convictions. As of March 2002, these proportions had barely changed, with the same kind of matters still respectively accounting for 39 and 54 percent of Bureau activity.
[35] "Protecting the Nation: The FBI in War and Peace"; Walker, *FBI Re-organization: Initial Steps Encouraging but Broad Transformation Needed*, 4-5.
[36] Markle Foundation, *Protecting America's Freedom*, pp. 76-78; Daly, "USA Centralises Terror Threat Assessments," 5; Corera, "Changes Needed in Information Sharing," 4. As Gordon Corera observes: "Because of the variety of information, departments and agencies involved, the question of which committee would exercise oversight remains problematic. The information includes but also goes far beyond the traditional provenance of committees such as Intelligence, Armed Services and Judiciary."
[37] In general terms, the Act: (1) prohibits disclosure by Federal agencies of any information contained in a system of records, except pursuant to a written request by or with the prior consent of the individual to whom the information pertains; (2) requires agencies that maintain and manage such record systems to keep account of disclosures of information and to inform the subjects of such disclosures when they occur; (3) allows record subjects to see and copy their information, establishes a procedure for amendment of such data and permits judicial review of any agency refusal to so amend; (4) requires that any information held be relevant to the agency's official purposes and be accurate; (5) mandates that agencies publish annual notices of the existence, character and accessibility of their record systems and that they take appropriate safeguards to maintain the confidentiality of such records; and (6) allows recordkeeping agencies to promulgate rules on all these matters. Markle Foundation, *Protecting American Freedom*, p. 128; Privacy Act of 1974, 5, United States Congress 552a(b) (1988).
[38] For more on this see Lillian BeVier, "Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection," *Bill of Rights Journal* 4/455, (1995). It is true that provision has been made for the DHS to have an Inspector General and possibly a Privacy Office. At the time of writing, the specific oversight roles of these various entities had not been spelled out nor had any delineation of their overall functional and jurisdictional remit been given.
[39] Fogarty and Ortiz, "Limitations Upon Interagency Information Sharing: The Privacy Act of 1974," 127. One of the most broadest interpretations of "routine use" was one proposed by the CIA, which sought the right to disclosure "whenever necessary or appropriate to enable the [Agency] to carry out its responsibilities." Congress objected to this interpretation as overly expansive and made a series of recommendations to narrow it. The CIA ignored these stipulations, however and published the routine use as planned.
[40] The USA Patriot Act was passed into law on October 26, 2001 and accorded sweeping new powers to both domestic law enforcement and international intelligence agencies involved in the fight against terrorism.

[41] Markle Foundation, "Protecting America's Freedom," p.90; "Push is On to Overhaul FBI," *Newsday*, December 29, 2002; The Electronic Frontier Foundation, "EEF Analysis of the Provisions of the USA PATRIOT Act That Relate To Online Activities," available on-line at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php

[42] For more on this point, see Chalk and Rosenau, *Confronting "the Enemy Within"*.

[43] Author's interview, CSIS, Ottawa, December 09, 2002.

[44] Author's interview with Los Angeles police official, 5 September 2003.

[45] Author's interview with Los Angeles police official, 5 September 2003.

[46] Markle Foundation, *Protecting America's Freedom*, 7p. 0.

[47] Brian Michael Jenkins, "Connects the Cops to Connect the Dots," *San Diego Union Tribune*, 1 June 2003, p. G1; and author's interview with senior US intelligence official, Arlington, VA, 6 August 2003.

[48] Progressive Policy Institute, "America at Risk: A Homeland Security Report Card," Washington, DC, July 2003, p. 12.

[49] In September 2002, the Justice Department's inspector general concluded that the FBI "has never performed a comprehensive written assessment of the risk of the terrorist threat facing the United States," although it had been promising to do so since 1999. US Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management," Report No. 02-38, September 2002, accessed at http: www.usdoj.gov/oig/audit/0238/exec.htm.

[50] Prior to 9/11, agencies contained in no less than four Cabinet-level departments had some role in domestic information gathering and assessment. Communication and collaboration between these various bureaus was un-integrated, subject to entrenched bureaucratic barriers and frequently confounded by entrenched jurisdictional jealousies.

[51] See, for instance, Markle Foundation, *Protecting America's Freedom*, pp. 71-72; "Center to Assess Terrorist Threat," *The Washington Post*, May 01, 2003.

[52] *Gilmore Commission Report*, p. 41; "Center to Assess Terrorist Threat," *The Washington Post*, May 01, 2003; "Terrorist Threat Data-Sharing Still an Ad Hoc Process," *Computer World*, July 22, 2003.

[53] U.S. General Accounting Office [GAO], *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened*, GAO-03-760 (Washington, DC: GAO, August 2003), fn. 30, p. 28.

[54] Author's interview with senior intelligence oficial, Arlington, VA, 6 August 2003.

[55] *Gilmore Commission Report*, p. 43; Markle Foundation, *Protecting America's Freedom*, p. 70; Jenkins, "Connect the Cops," p. G1.