BEYOND CONNECTING THE DOTS:

A VITAL FRAMEWORK FOR SHARING LAW ENFORCEMENT INTELLIGENCE INFORMATION

AN INVESTIGATIVE REPORT BY THE

U.S. House Committee on Homeland Security Democratic Staff

Prepared for Congressman Bennie G. Thompson, Ranking Member

Introduction

The 9/11 attacks demonstrated that the terrorists who intend Americans harm do not always live overseas in faraway lands. Some reside among us in our cities and towns where they can test our nation's vulnerabilities and plot their next strike with relative ease. In the face of this threat, the hundreds of thousands of law enforcement officers across the country offer the best hope for detecting and preventing terrorist attacks before they happen.

In the course of their day-to-day work, these officers observe activities and conditions that may be indicators of an emerging terrorist plot. For example, because terrorists typically commit crimes when preparing to carry out their attacks, local law enforcement may interact with them during the course of otherwise ordinary criminal investigations. Such interaction thus presents a critical opportunity to intercept terrorists before they strike. Providing officers with the specific and actionable law enforcement intelligence they need to identify both terrorists in their midst and the particular threats they pose, however, remains a continuing challenge.

Despite numerous directives, exhortations, and invitations to do so, federal policymakers have failed to develop uniform standards for converting classified intelligence into an unclassified or "less classified" format that can be disseminated rapidly to appropriate state, local, and tribal authorities to thwart terrorist attacks. They likewise have failed to create effective mechanisms through which the particular intelligence needs of those authorities can be voiced and met, or where their own information assets can be shared with the Intelligence Community (IC).

This distressing lack of leadership has persisted for more than four years. In an effort to move the IC from a Cold War era "need to know" mentality to a "need to share" mindset responsive to today's threats, Congress passed the Homeland Security Act of 2002 (Homeland Security Act).[1] The Act directed the President to develop procedures for the declassification and dissemination of intelligence information and recommended several possible approaches. It took nearly seven months before an Executive Order took the small step of delegating this responsibility to the Department of Homeland Security (Department).[2] When the Department failed to act, President Bush issued a new Executive Order more than a year later directing all federal agencies possessing or acquiring terrorism information to assist the Director of Central Intelligence (DCI) in developing common standards for information sharing – including standards that addressed the conversion of classified intelligence into an unclassified or "less classified" format.[3] Still nothing happened. Congress subsequently tried to prod the process along with the Intelligence Reform and Terrorism Prevention Act of 2004 (9/11 Act), directing the new Director of National Intelligence (DNI) to establish uniform means and methods

[1] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2155 (2002) [hereinafter Homeland Security Act].
[2] Exec. Order No. 13,311, 68 Fed.Reg. 45149 (July 31, 2003) [hereinafter Exec. Order No. 13,311].
[3] Exec. Order No. 13,356, 69 Fed.Reg. 53599 (Sept. 1, 2004).

for this purpose.[4] It was not until April 2005, however, that the President actually appointed a Program Manager to take on this task.[5] Since that time, the Program Manager has made little progress in harmonizing the disparate approaches to declassification within the IC. Residual cultural resistance to information sharing between the various federal intelligence agencies has only compounded the problem.

Clearly, the current approach is not working. Rather than pursuing this patchworked approach, the United States would be better served by a solution modeled on the Central Services' Police International Counter Terrorism Unit (PICTU) and the Security Service's Joint Terrorism Analysis Centre (JTAC) in the United Kingdom (UK).[6] JTAC, with PICTU's assistance, has established a successful process by which highly classified intelligence information is converted to a law enforcement sensitive-type format that can be widely disseminated to police officers to support both threat assessment and prevention planning.[7] JTAC is staffed not only by intelligence analysts but also by a select group of police officers with security clearances – including representatives from PICTU – who know firsthand what information their colleagues in the field need to intercept terrorists and foil their plans.[8] JTAC, with PICTU's assistance, can identify what intelligence information would be of interest at a local level, redact whatever portions of that information might harm the national security, and funnel it to an appropriate audience. In addition to the critical role that PICTU plays in this process, it also uses open source material to inform local police forces of terrorist threats and how to address them when intelligence resources are lacking.

Our country already has a JTAC equivalent in the newly-established National Counterterrorism Center (NCTC), a national hub for intelligence analysis under the

---

[4] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, Title I § 1016(a)(2), 1016(f)(1), (2), 118 Stat. 3638 (2004) [hereinafter 9/11 Act].

[5] In its March 31, 2005 report, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction recommended that the ISE Program Manager should report to the DNI. **Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States** 28 (March 31, 2005) [hereinafter Robb-Silberman Report], available at http://www.wmd.gov/report/wmd-report.pdf. On June 2, 2005, President Bush accordingly issued a directive stating that the DNI would have "authority, direction and control" over Russack. See Press Release, the White House, Memorandum for the Heads of Executive Departments and Agencies; Subject: Strengthening Information Sharing, Access, and Integration B Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment (June 2, 2005) at http://www.fas.org/sgp/news/2005/06/wh060205.html. This move addressed what one observer had called the "confused lines of responsibility for information sharing with in the intelligence community" that had existed until that time. Chris Strohm, "Bush Directive Clarifies Information Sharing Responsibility," Govexec.com (June 3, 2005), at http://www.govexec.com/story_page.cfm?articleid=31404&printerfriendlyVers=1&.

[6] Email from Keith Weston, Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Sept. 1, 2005, 10:56:00 EDT) [hereinafter Weston Sept. 1 Email] (on file with author).

[7] Id.; Keith Weston, New Threshold Terrorism – A UK Perspective 5 (January 2005) [hereinafter New Threshold Terrorism Manuscript] (unpublished manuscript, on file with author).

[8] Email from Keith Weston, Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Aug. 19, 2005, 04:34:00 EDT) [Weston Aug. 19 Email] (on file with author).

leadership of the DNI where executives and experts from across the IC work side-by-side under the same roof to instantly pool their information, analyze data, draw conclusions from it, and then to plan, coordinate, and direct national counterterrorism operations in response.[9] Nevertheless, we lack a PICTU-like mechanism that not only is responsive to the concerns and needs of law enforcement on a jurisdiction and threat-specific basis but also bypasses the cultural turf wars that continue to plague the IC. A Vertical Intelligence Terrorism Analysis Link (VITAL) unit collocated at the NCTC and staffed with a broad cross-section of representatives from state, local, and tribal law enforcement would:

(1) inform the intelligence analysis process by identifying intelligence information that would be of interest to officers conducting operational and strategic planning;

(2) assist in the dissemination of both sanitized intelligence products and open source-based informational products to the appropriate police audience; and

(3) educate not only the IC about law enforcement's particular needs but also front line officers about the IC's homeland security plans and priorities.

VITAL would not only help avoid indiscriminate data dumps that can overload and overwhelm local authorities but also would provide a key channel for those authorities to share information with their federal partners.

The Federal Government's Failure to Effectively Lead Law Enforcement Intelligence Information Sharing Strategies

In the Homeland Security Act, Congress recognized that the federal government relies on state, local, and tribal law enforcement officers to protect the nation against terrorist attacks, and that they consequently require at least "some homeland security information," or law enforcement intelligence,[10] in order to prevent and prepare for such

[9] Federal Bureau of Investigation Home Page, The National Counterterrorism Center: Bringing Down the Walls of Information Sharing . . . Literally, Aug. 29, 2005, at http://www.fbi.gov/page2/aug05/nctc082905.htm.

[10] "Law enforcement intelligence" is defined as "the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at both the tactical and strategic levels." See David L. Carter, Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies; Chapter 2: Understanding Current Law Enforcement Intelligence: Concepts and Definitions 11 (November 2004) (citations omitted), available at htttp://www.cops.usdoj.gov/mime/open.pdf?Item=1393. Law enforcement intelligence falls into two categories: (1) policy intelligence, which is concerned with threatening actions and activities of entities hostile to the United States; and (2) military intelligence, which focuses on hostile entities, weapons systems, warfare capabilities and order of battle issues. Id. at 14 (citations omitted). A third category of intelligence, national security intelligence, includes both policy and military intelligence. Id.

incidents.[11] Congress noted that the need to convey such information – which at times could be of a classified or sensitive nature – must be reconciled with the need to preserve and protect the intelligence sources and methods used to acquire that information.

In order to initiate the process, Congress required the President to prescribe and implement procedures under which the IC[12] could (1) share relevant and appropriate homeland security information with appropriate state and local personnel; (2) determine – to the extent that that information includes classified data – whether, how, and to what extent such data should be removed in order to promote information sharing; and (3) share classified or otherwise protected homeland security information with state and local personnel under appropriate circumstances.[13] Congress likewise recommended three potential methods to promote this flow of this information: (1) providing security clearances to appropriate state and local officials; (2) entering into nondisclosure agreements regarding sensitive but unclassified information with such officials; and (3) increasing the use of information sharing partnerships that include such officials – such as the Department of Justice's Joint Terrorism Task Forces (JTTFs) and Anti-Terrorism Task Forces (ATTFs) and regional Terrorism Early Warning Groups (TEWs).[14] Congress likewise recognized that "[m]ethods exist to declassify, redact, or otherwise adapt classified information so it may be shared with state and local personnel" and urged that those methods be pursued as well.[15]

Federal policymakers have long paid lip service to these various approaches. Despite numerous strategy pronouncements, memoranda of understanding, Executive Orders, reports, and promised guidelines for how to "do" information sharing, they nevertheless have come up short time and time again. To date, there is no consistent, effective method to convert classified law enforcement intelligence into a specific, actionable, and unclassified or lower classified format that might inform terrorism prevention efforts. There likewise is no mechanism to rapidly target that information to appropriate officers in the field. A chronology of the lack of progress in this area over the last several years suggests a serious lack of commitment to achieving these critical homeland security goals:

---

[11] Homeland Security Act, § 891(b)(2), (4). The Homeland Security Act defines "homeland security information" as "any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist organization; or (D) would improve the response to a terrorist act." Id., Title VIII § 892(f)(1). For ease of use, this report will use the terms "law enforcement intelligence" and "homeland security information" interchangeably.

[12] The IC traditionally has included the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office, as well as the intelligence components of the Federal Bureau of Investigation (FBI), Department of State, Department of Treasury, Department of Energy and the respective military services. The Department of Homeland Security is the newest addition to the IC.

[13] Homeland Security Act at § 892(a)(1)(A), (C); (c)(1).

[14] Id. at § 892(c)(2)(A), (B), (C).

[15] Id., § 891(b)(6), (7).

July 2002

In July 2002, President Bush first touched on the issue of information sharing in his National Strategy for Homeland Security, stating that he would lead a review of all authorities governing the analysis, integrity, and disclosure of intelligence with the goal of improving information sharing at all levels of government through legislative reform.[16] Toward that end, the President asserted that the federal government would work to remove classified information from some documents to facilitate distribution to more state and local authorities.[17] "The effort," he stated, "will help state and local law enforcement officials learn when individuals suspected of criminal activity are also under federal investigation and will enable federal officials to link their efforts to investigations being undertaken in the states."[18]

February 2003

President Bush repeated his promise in February 2003 when unveiling his National Strategy for Combating Terrorism, stating, "The Intelligence Community and law enforcement agencies will therefore continue their aggressive efforts to identify terrorists and their organizations, map their command and control and support infrastructure, and then ensure we have broad, but appropriate, distribution of the intelligence to federal, state, and local agencies as well as to our international allies."[19] The National Strategy for Combating Terrorism specifically referred back to the National Strategy for Homeland Security as a model for adapting information sharing techniques developed domestically to the international arena:

> *The National Strategy for Homeland Security addresses information sharing and technology within the United States. The components of this information sharing apply equally well at home and abroad. Those procedures and systems that facilitate interagency, intergovernmental, and private information sharing will be expanded to allow our overseas agencies to have access and input, as necessary. This initiative will include not only database alignment and the horizontal and vertical information flow; it will also optimize disclosure policy and establish consistent reporting criteria across agencies and allies.*[20]

At the same time he unveiled his National Strategy for Combating Terrorism, the President also issued his National Strategy for the Physical Protection of Critical

---

[16] George W. Bush, The National Strategy for Homeland Security 48 (Washington, D.C., The White House, July 2002), available at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
[17] Id. at 57.
[18] Id.
[19] George W. Bush, The National Strategy for Combating Terrorism 16 (Washington, D.C., The White House Feb. 2003), available at http://www.whitehouse.gov/news/releases/2003/02/20030214=7.html.
[20] Id. at 26.

Infrastructure and Key Assets.[21] Building upon his previous statements, President Bush bemoaned the lack of a coordinated, integrated mechanism that could strip intelligence of sensitive details and then distribute the sanitized version of documents to a targeted audience:

> *If intelligence sources and methods are omitted, many intelligence reports may be declassified. Time-efficient procedures are needed to declassify relevant intelligence or extract information from classified sources and disseminate that information to the appropriate recipients. These concerns are complicated by the ineffective means by which sensitive information is transferred, as well as the mechanisms currently in place to ensure that required information is disseminated appropriately. Currently, there is no central, coordinating mechanism to assess the impact of sensitive information and ensure that it gets to all the parties with a need to know. Adding to this problem is the lack of technical communications systems to enable the secure transmittal of classified threat information to the owners and operators of concern.*[22]

The President concluded that the inherent lack of trust among key stakeholders also impeded effective information sharing, adding, "Without all pieces of the information puzzle, we operate from a major disadvantage in the fight against terrorism."[23]

Having acknowledged these difficult problems, it was incumbent upon the President to lead a solution. Instead, he delegated the task of addressing them to agencies, offices, and people who either could not or would not do the hard work necessary to implement change.

March 2003

Shortly thereafter in March 2003, Attorney General John Ashcroft, DCI George Tenet, and Department Secretary Tom Ridge entered into a Memorandum of Understanding (MOU) that provided a "framework and guidance to govern information sharing, use, and handling."[24] Among other things, the MOU signatories agreed to make intelligence information available to the Department – then seen as the logical conduit of information to state, local, and tribal law enforcement – "promptly" and "in a manner, and through mechanisms" that protected both sources and methods.[25] The Attorney General and the DCI agreed to make such information available "in a form suited to [the

---

[21] George W. Bush, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, (Washington, D.C., The White House, Feb. 2003) [hereinafter Critical Infrastructures Strategy], available at www.whitehouse.gov/pcipb/physical/html.
[22] Id.
[23] Id.
[24] George J. Tenet, Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing 1 (March 4, 2003), available at http://www.fas.org/sgp/othergov/mou-infoshare.pdf.
[25] Id. at 16-17.

Department's] effective use of that information . . ."[26] Both promised to ensure "that dissemination is done in a manner that ensures the broadest possible availability."[27] To meet those obligations, the Attorney General and the DCI committed to redacting sources and methods from intelligence documents and to creating "tailored products" that excluded those details.[28] The MOU signatories likewise agreed to adopt "sanitization" methods, as well as protocols to modify classification levels, in order to provide law enforcement with the information it needs.[29] Finally, the signatories pledged to use "high-content 'tear lines' suitable for onward passage at an unclassified level."[30] They agreed to "ensure, to the greatest extent possible, that covered entities utilize agreed-upon standardized formatting for preparation of tear-line material for passage to state, local, or private sector officials . . ."[31]

The MOU was devoid of policies or procedures regarding exactly how or what to redact from documents to be disseminated to law enforcement; what common standards should govern the creation of "tailored products" for that audience; or how unclassified tearline documents should be prepared. The signatories instead agreed "to develop together, as soon as practicable, mechanisms and procedures, including through the use of detailees and assignees to the TTIC [Terrorist Threat Integration Center] and JTTFs, as appropriate" to carry out these provisions.[32] In the interim, the signatories established a case-by-case procedure for Department officials to ask the particular agency that developed a specific classified document – on an as needed basis – to (1) declassify or reduce the classification level of the document in question; or (2) provide an "alternative formulation" of the document in question without declassifying it or reducing its classification level.[33] The MOU signatories apparently never took further action, however, and the "interim" procedure they adopted has lasted to this day.

July 2003

In July 2003, President Bush signed Executive Order 13311 which delegated his authority to establish government-wide information sharing procedures to Department Secretary Tom Ridge.[34] Executive Order 13311 made clear that any such procedures were to apply "to all agencies of the Federal Government" – providing the Secretary with the opportunity to completely revamp how the IC does business.[35] Despite the chance to

---

[26] Id. at 17.
[27] Id.
[28] Id.
[29] Id.
[30] Id. "Tear line" reports are reports produced by an intelligence agency in which includes a classified version of information with a "less classified" or unclassified version immediately below it under a "tear-line" or conspicuous fold. See **Markle Found., Creating a Trusted Information Network for Homeland Security, Second Report of the Markle Foundation Task Force** 40 n.24 (2003) [hereinafter "**Markle Foundation Second Report**"]. Because the version below the tearline excludes sources and methods information, it can be more easily shared with state, local, and tribal law enforcement officers.
[31] Id.
[32] Id. at 18.
[33] Id.
[34] Exec. Order No. 13,311, supra note 2.
[35] Id., Section 1(c).

lead critical policy development in this area, the Secretary failed to act. As the Congressional Research Service (CRS) noted earlier this year, "While many observers expected that these procedures would be issued during the summer of 2004, they have not appeared to date."[36]

June - August 2004

Federal policymakers apparently lost faith in the Department's ability to fulfill this mandate. In August of last year, the President issued Executive Order 13356, which reassigned the task of establishing uniform information sharing procedures to the DCI and required their completion within ninety (90) days.[37] The President recommended "common standards" to guide the DCI's work which, among other things, included (1) requiring intelligence agencies – at the outset of the intelligence collection and analysis process – to create unclassified versions of intelligence reports and/or versions of such reports that protect sources and methods; (2) requiring intelligence records to be available at multiple levels of classification – to be accessed through an electronic "tearline" system – so that intelligence personnel could review whatever information was appropriate given their particular security clearance level; and (3) minimizing the use of "originator controls" that give agencies that originate a piece of intelligence information the final say-so about who can review that information.[38] Despite these suggestions and President Bush's November 25, 2004 deadline for the completion of this work, the DCI never issued the required policies.

This failure was particularly troubling given the statements of William F. Dawson, the Deputy Intelligence Community Chief Information Officer, during the period leading up to passage of the 9/11 Act.[39] Dawson announced at an information sharing symposium during the summer of 2004 that the DCI had recently established a mandatory write-to-release policy that required intelligence agencies to generate – at the outset of intelligence collection – unclassified or "less classified" versions of intelligence documents that could be disseminated widely.[40] This new mandate, he added, was to be implemented by using new technologies that would generate tearlines automatically.[41] Dawson further stated that the DCI planned to enforce the policy by taking program funding away from those officials who failed to comply.[42] Furthermore, he asserted that the DCI intended to establish a new organization that would rule on disagreements

---

[36] Harold C. Relyea and Jeffrey W. Seifert, Information Sharing for Homeland Security: A Brief Overview, **Congressional Research Service**, Jan. 10, 2005, CRS 18.

[37] Exec. Order No. 13,356, supra note 3. See Letter from David M. Walker, Comptroller General of the United States, to the Honorable Tom Davis, Chairman, House Committee on Government Reform (Sept. 9, 2004) at http://www.gao.gov/decisions/other/303692.htm.

[38] Id., Sec. 3(a)-(c). Minimizing the use of originator controls would help avoid the situation where, for example, the FBI is not be able to share with local law enforcement originator controlled intelligence information that it had received from the CIA without the CIA's prior consent

[39] Wilson P. Dizard III, "New Entity to Govern Information Sharing," GCN.com (June 29, 2004), at http://www.gcn.com/vol1_no1/daily-updates/26416-1.html.

[40] Id.

[41] Id.

[42] Wilson P. Dizard III, "Intelligence Office Will Enforce 'Right to Release' Policy," GCN.com (July 5, 2004), at http://www.gcn.com/23_17/news/26467-1.html.

between agencies over sharing classified information.[43] One journalist quoted Dawson as saying, "'If the [National Security Council] wants information from the FBI and the FBI says no, there is going to be an organization' to rule on the dispute . . ."[44]

Despite these lofty policy promises, however, the DCI never issued a single, mandatory write-to-release policy that included criteria prescribing how the IC should prepare unclassified or "less classified" versions of intelligence documents. Specifically, the DCI never issued clear guidelines explaining how the IC should excise source and method information in a way appropriate to particular intelligence consumers. The DCI likewise never created an automated mechanism capable of generating tearlines in the way Dawson described. Finally, the DCI never established an organization to arbitrate information sharing disputes.

December 2004

Sensing this lack of progress, Congress tried to advance the agenda through the 9/11 Act – requiring the President to (1) establish an Information Sharing Environment (ISE) designed to facilitate the sharing of terrorism information; and (2) appoint a Program Manager who would assist in the development of information sharing "policies, procedures, guidelines, rules, and standards" to "foster the development and proper operation of the ISE . . ."[45] Congress further required the President – by September 13, 2005 – to issue "guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained . . ."[46] Congress also sought to bring the newly created DNI into the mix, directing him to establish and implement guidelines for the "[p]reparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable."[47] Early signs from John A. Russack, the ISE Program Manager who President Bush named in April 2005 and who he ultimately appointed to create the aforementioned guidelines, were not promising.[48]

June 2005

The 9/11 Act required Russack to (1) prepare a preliminary report by June 15, 2005, that included a description of the technological, legal, and policy issues presented by the creation of the ISE and the way in which those issues would be addressed;[49] (2)

---

[43] Id.
[44] Id.
[45] 9/11 Act, supra note 4 at Title I § 1016(a)(2), 1016(f)(1), (2).
[46] 9/11 Act, § 1016(d)(1). This section specifically required that the guidelines were to be generated "in no event no later than 270 days after the date of the enactment of this Act . . ." September 13, 2005, marked the 270th day from the 9/11 Act's December 19, 2004 enactment date.
[47] Id. § 1011(i)(2)(C).
[48] Robb-Silberman Report, supra note 5 at 28; Press Release, supra note 5; Strohm, supra note 5.
[49] Despite the Program Manager's clear policy development role in this area, the President recently advised that on June 2, 2005, he established the Information Sharing Policy Coordination Committee (ISPCC) – an

establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating within the federal government intelligence and terrorism information and people with relevant knowledge about same; and (3) conduct a review of relevant current federal agency capabilities, databases, and systems for sharing information.[50] Although Russack submitted a ten-page "Preliminary Report on the Creation of the Information Sharing Environment" by the June 15th deadline, it fell considerably short of those requirements.[51] For example, the report offered up little detail in the three-and-one-half pages it devoted to "several key issues" that Russack identified as having arisen with the advent of the ISE.[52] It likewise promised that Russack and his staff would analyze, review, and work toward solutions of those issues – without identifying specific steps that might be taken to address them.[53] Furthermore, the report addressed the directory services issue in only two paragraphs, clarifying one thing only: the Program Manager had failed to establish an initial capability for those services.[54] Russack instead promised to "assess current or planned investments" in directory services that were/might be underway.[55] Finally, the report was silent about Russack's obligation to conduct a review of current federal agency capabilities for information sharing – deferring instead to the Office of Management and Budget's own initiatives in this regard.[56]

July 2005

The reason for Russack's rather thin preliminary report became apparent during his testimony before the Senate Judiciary Committee on July 27, 2005. In his opening statement to that committee, Russack explained that in order to develop guidelines that would enable greater information sharing with "state, local, tribal, and private sector

---

entity chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC) – which he described as "the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM [Program Manager], and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses." Memorandum from President George W. Bush to the Heads of Executive Departments and Agencies (Dec. 16, 2005) [December 16 Memorandum], available at http://www.whitehouse.gov/news/releases/2005/12/print/20051216-10.html. Despite the ISPCC's apparent centrality to the process, it was the Program Manager who developed the below described information sharing guidelines that the White House released on December 16, 2005. Id.

[50] 9/11 Act, § 1016(c).

[51] **Information Sharing Program Manager, Preliminary Report on the Creation of the Information Sharing Environment** 4 (June 15, 2005) (on file with author).

[52] Id. at 4-8. Those issues included (1) ambiguous and conflicting authorities and policies governing roles and responsibilities of departments and agencies participating in the ISE; (2) a lack of trust among organizations when sharing information; (3) the inability of authorized ISE users to obtain timely access to terrorism-related information as a result of originator controls, requirements, and restrictions; (4) the need to protect privacy and other legal rights; and (5) the need to remove technology barriers to information sharing.

[53] Id.

[54] Id. at 8.

[55] Id.

[56] Id. at 8-9.

officials,"[57] he would be assisted by "a very small staff of approximately 25 people" – most of whom would be detailees from other government agencies.[58] In response to questioning from Senator Arlen Specter, however, Russack conceded that as of the date of the hearing, he had been provided only one full-time employee and two contractors to assist him with his work.[59] Senator Specter expressed his concern about this apparent lack of urgency, asking, "If I were to write a scathing letter, [to] whom would I address it to give you some help?"[60] Russack responded that Senator Specter should write the DNI and that he (Russack) would accept whatever additional help could be provided.[61]

September 2005

In anticipation of the new information sharing guidelines, the Markle Foundation – the author of a well-respected study on the subject – wrote to President Bush on September 7, 2005, to express its concerns regarding its slow progress and offered suggestions about how the government could move forward with developing effective policies in this area.[62] While acknowledging that the President's Executive Orders and the 9/11 Act had generated "genuine progress toward creating an Information Sharing Environment (ISE)," the authors expressed concern not only about the apparent resistance to change in some quarters but also the lack of urgency about taking steps to make the ISE a reality:

> *We remain concerned, however, that risk aversion and bureaucratic resistance to change continue to hamper the carrying out of announced new policies. The constitutional and statutory authorities to do what needs to be done exist. We urge you to reiterate to your Cabinet officers and all U.S. Government officers that they should interpret all applicable laws and regulations to enable information sharing rather than use ambiguities in the Act and prior law which Congress left unresolved as an excuse to protect prior approaches. They need to embrace rather than resist the change.*
>
> *It is our view that we as a nation must move to create the ISE with great urgency, and that we should not be satisfied with the first steps – as major as they are – that have been taken in the four years since the 9/11 attacks. The same sense of urgency and focused attention exercised by our military men and women in the battlefield must be applied to reforming how*

[57] U.S. Congress. Senate. Committee on the Judiciary. Hearing on FBI Oversight. 109th Cong., 1st sess., 2005 (Congressional Quarterly Transcript on file with author).
[58] Id.
[59] Id.
[60] Id.
[61] Id.
[62] Letter from Zoe Baird and Jim Barksdale, Co-Chairs of the Markle Task Force on National Security in the Information Age, to the President of the United States (Sept. 7, 2005) (on file with author). See U.S. Government Accounting Office, Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened, GAO-03-760, (Washington, D.C.: GAO, August 2003), 33.

government agencies work together to understand and prevent the threats to the nation.[63]

Among the Markle Foundation's recommendations was a greater, immediate emphasis on the development of government-wide policies as the foundation for the adoption of information sharing capabilities and procedures.[64] "Sweeping change is needed to remove any pre-9/11 confusion about information sharing that, regrettably, still exists in some departments and agencies," the authors continued.[65] "A single set of policies across the government, while recognizing the need for some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations."[66]

October 2005

On October 21, 2005, the Administration responded that the Markle Foundation should "rest assured" that the DNI "fully appreciates his responsibility with respect to creating the ISE, and will ensure the Program Manager – who is subject to the DNI's authority, direction and control – receives the support he needs."[67] Rather than issuing actual "guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form,"[68] however, the officials signaled for the first time that President Bush would be releasing some sort of generalized directive "*designed* to set Government-wide policies and procedures" in this area.[69] In other words, he appeared poised to issue guidelines to create guidelines rather than to meet his statutory obligation of setting specific information sharing policies and procedures applicable to the IC.

On October 25, 2005, the President rescinded Executive Order 13356 and replaced it with Executive Order 13388, entitled, "Further Strengthening the Sharing of Terrorism Information to Protect Americans."[70] The Executive Order appeared to adopt the President's aforementioned "common standards" for the development of information sharing guidelines set forth in Executive Order 13356 – but this time *as actual information sharing guidelines*, at least until he issued the promised directive.[71] Executive Order 13388 likewise established the Information Sharing Council (ISC) prescribed by the 9/11 Act.[72] The ISC includes designees of the Secretaries of Commerce, Defense, Energy, State, Treasury, and Homeland Security; the Attorney

---

[63] Id.
[64] Id. at 2.
[65] Id.
[66] Id.
[67] Letter from Stephen J. Hadley, Assistant to the President for National Security Affairs, and Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, to Zoe Baird, Co-Chairman of the Markle Task Force on National Security in the Information Age (Oct. 21, 2005) (on file with author).
[68] 9/11 Act, § 1016(d)(1).
[69] Hadley, supra note 67 (emphasis added).
[70] Exec. Order No. 13,388, 70 Fed. Reg. 207 (Oct. 27, 2005).
[71] Id.
[72] Id.

General; the DNI; the CIA Director; the Director of the Office of Management and Budget; the FBI Director; the NCTC Director; and others.[73] According to Executive Order 13388, the ISC is supposed to provide advice and information concerning the establishment of an "interoperable terrorism information sharing environment and, among other things, to conform approaches and technologies for this purpose across agencies."[74]

Notably, Section 1016(g) of the 9/11 Act provides that designees to the ISC are to serve two-year terms "beginning on the date of the initial designation of the program manager . . ."[75] As discussed previously, President Bush designated Russack as the Program Manager on April 15, 2005. By waiting until October 25, 2005, to formally establish the ISC, the President effectively deprived the designees of more than six months of their two-year terms.

December 2005

The October 21, 2005 letter to the Markle Foundation proved prophetic. On December 16, 2005 – more than three months after finalized information sharing guidelines were due under the 9/11 Act – the President issued a Memorandum which, among other things, sets forth five guidelines to create guidelines.[76] Instead of breaking new ground, they simply restate the undisputed need to: (1) define common standards for how information is acquired, accessed, shared, and used within the ISE; (2) develop a common framework for the sharing of information between and among executive departments and agencies and state, local, and tribal governments, law enforcement agencies, and the private sector; (3) standardize procedures for sensitive but unclassified information; (4) facilitate information sharing between executive departments and agencies and foreign partners; and (5) protect the information privacy rights and other legal rights of Americans.[77] In addition to rehashing these obvious challenges, the Memorandum also announces that the President plans to take another ninety (90) days to produce something more substantive.[78] Specifically, it directs the Attorney General, the DNI, and the Secretaries of Defense, State, and Homeland Security to "develop and issue . . . common standards":

> *(i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use and disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that*

---

[73] Id. See also Patience Wait, "Executive Order Bolsters Information Sharing Among Agencies," GCN.com (Oct. 27, 2005), at http://www.gcn.com/vol1_no1/daily-updates/37432-1.html.
[74] Exec. Order No. 13,388, 70 Fed. Reg. 207 (Oct. 27, 2005).
[75] 9/11 Act, § 1016(g).
[76] December 16 Memorandum, supra note 49.
[77] Id.
[78] Id.

include the appropriate method for the Government-wide adoption and implementation of such standards.[79]

"Such standards," the Memorandum continues, "shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector."[80] It further announces that federal policymakers need an additional ninety (90) days after the development of these standards to "jointly disseminate" them for use by state, local, and tribal law enforcement agencies "on a mandatory basis where possible and a voluntary basis where not."[81] The Memorandum likewise advises that a recommended framework to govern executive roles and responsibilities for sharing law enforcement intelligence information with those agencies is at least 180 days away.[82]

* * *

If all this sounds familiar, that is because it is. At bottom, federal policymakers have failed to advance the information sharing agenda in any meaningful way. Despite a tremendous amount of talk, we still do not have uniform guidelines or standards for converting classified law enforcement intelligence into an unclassified or "less classified" format that can be disseminated rapidly to our front line officers who need it most. Moreover, we still do not have mechanisms through which the particular intelligence needs of those officers can be consistently voiced and met, or where their own information assets can be shared with the IC. The assignment and re-assignment of work to address these shortcomings have too often resulted in a game of homeland security "hot potato" that has deferred needed solutions to another day. Recent terrorist attacks in Europe and elsewhere demonstrate that we have no more time to waste. Before plunging headway into another well-meaning legislative solution to the problem, however, it is important to review which information sharing approaches have enjoyed at least some success and which have not.

Sharing Law Enforcement Intelligence: Tested Alternatives Fail to Provide Officers With the Information They Need

As noted previously, Congress in the Homeland Security Act suggested three possible options for federal policymakers to consider when designating an information sharing process: (1) providing security clearances to appropriate state and local officials; (2) entering into nondisclosure agreements regarding sensitive but unclassified information with such officials; and (3) increasing the use of information sharing partnerships that include such officials – such as JTTFs, ATTFs, and TEWs. For a variety of reasons, none of these mechanisms are sufficient for ensuring the consistent

[79] Id.
[80] Id.
[81] Id.
[82] Id.

flow of law enforcement intelligence information that police and sheriffs' officers nationwide need to identify terrorists and to thwart terrorist attacks in their communities.

Security Clearances for All?

The Homeland Security Act states that "[g]ranting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government."[83] Shortly after the Act's passage, Frederick M. Kaiser of CRS described the perceived need for a consistent, government-wide security clearance policy that could promote information sharing:

> *Because of the absence of standardized security clearance requirements, high-ranking state and local public officials – mayors, municipal chiefs of police, county executives, sheriffs, and even governors, in some instances – have been denied certain information; and those who have received it may not have been able to share it with their colleagues, even officials who otherwise outranked or supervise them. This condition has existed, in large part, because their need for classified national security information has been narrow and circumscribed – confined, for instance, to nuclear weapons facilities or certain defense establishments within their jurisdictions. The heightened priority to combat terrorism, by contrast, has broadened the boundaries.*[84]

Many state and local officials were initially supportive of expanding access to security clearances in order to obtain law enforcement intelligence. For example, the National Governors Association's Center for Best Practices argued that, "Granting security clearances to certain state and local personnel using a compartmented, need-to-know system would facilitate secure sharing of critical intelligence. Security clearances should be standardized and reciprocal among agencies and levels of government."[85] The U.S. Advisory Panel on Terrorism – composed of former federal and state and local officials experienced in public safety matters – were likewise broadly supportive of this approach.[86]

The FBI accordingly established the State and Local Law Enforcement Executives and Elected Officials Security Clearance Initiative, which was designed, among other things, to grant security clearances in order to "help ensure the free flow of information between the FBI and state and local law enforcement

---

[83] Homeland Security Act, §§ 891(b)(6); 892(c)(2)(A).
[84] Frederick M. Kaiser, "Access to Classified Information: Seeking Security Clearances for State and Local Officials and Personnel," Government Information Quarterly 20 (2003) at 215.
[85] Id. (citing National Governors Association, NGA Center for Best Practices, States' Homeland Security Priorities Issues Brief 2 (Aug. 19, 2003)).
[86] Id. (citing U.S. Advisory Panel to Assess Domestic Response Capabilities for Combating Terrorism IV, Implementing the Strategy: Advanced Recommendations on Strategy and Structure for the Fourth Annual Report (2002) at www.rand.org/organization/nsrd/terrpanel.

officials."[87] Complementing this effort, the Department sponsored its own State & Local Security Clearance Program in order to "meet the need of certain officials for classified material"[88] including the Department's state and local homeland security partners such as "[p]ersonnel who work in law enforcement."[89] Nevertheless, most of the hundreds of thousands of state, local, and tribal police and sheriffs' officers throughout the country have not taken advantage of either program. Between 9/11 and October 2005, only 6,011 law enforcement "executives" and JTTF members have been provided with security clearances through the FBI program.[90] As of June 2005, moreover, only 325 state and local government officials had been vetted for DHS-sponsored Secret and Top Secret-level security clearances, with an additional 250 state and local government officials in various stages of processing for a Secret-level clearance.[91]

This situation is not surprising. As the Department of Justice's Office of the Inspector General (DOJ OIG) first noted two years ago:

> *The process for obtaining a security clearance is cumbersome and time consuming and a process over which the FBI has little control. The application forms are the same ones that federal employees use, including FBI agents, when applying for a security clearance. The forms are lengthy and detailed. For example, applicants are required to list their residences for the last seven years along with details on education, employment, foreign travel, and other data. After the forms are completed, background investigations are conducted on each applicant. These background investigations are mandated by Presidential Executive Order. Compounding the expense and time required to grant a security clearance to a state or local law enforcement official is the perception, according to the Police Executive Research Forum, by some state and local officials that they should not have to undergo the same background investigation process as other people who receive security clearances. FBI officials told us that some state and local law enforcement executives think that their position alone demonstrates their trustworthiness.*[92]

David L. Carter of the School of Criminal Justice at Michigan State University echoed these sentiments, adding that an "open application" approach under which all law

---

[87] U.S. Government Accounting Office, Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials, GAO-04-596, (Washington, D.C.: GAO, April 2004), 2.
[88] Department of Homeland Security, Fact Sheet: State & Local Security Clearance Program (Nov. 12, 2003), available at http://www.scd.state.hi.us/CSSPrototype/portallist/SL_Clearance_Fact_Sheet.doc.
[89] Id.
[90] E-mail from James R. Blanchard, FBI Office of Congressional Affairs, to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Nov. 18, 2005, 09:33 EST) (on file with author).
[91] E-mail from Michael Cappannari, Legislative Assistant, Office of Legislative Affairs, Department of Homeland Security, to Frederick M. Kaiser, Specialist in American National Government, Government and Finance Division, Congressional Research (June 3, 2005, 11:03 EDT) (on file with author).
[92] United States Department of Justice, Office of the Inspector General, Audit Division, The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information 14 (Dec. 2003) (citation omitted).

enforcement officers everywhere could obtain security clearances would not only place classified information into too many hands but also would be cost and time prohibitive:

> *First, security clearance means having access to classified information. Before authorizing the application for a clearance, the agency should assess the applicant's "right to know" and "need to know" classified information . . . It may be reasonable to grant a security clearance to a local police detective who works organized crime cases; however, a traffic commander would have virtually no need for a clearance.*
>
> *Second, the clearance process is labor intensive and expensive. It is simply not prudent fiscal management to authorize clearance investigations in all cases. Third, conducting an excess number of clearance investigations slows the process, thereby taking longer to process clearances for those persons who may be in more critical positions.* [93]

In its June 2005 review of the Department of Justice's terrorism task forces, moreover, the DOJ OIG described lingering opposition by some law enforcement officers to having to subject themselves to the vetting process:

> *One local official we interviewed was not as positive about the sharing of information by the FBI. A Sheriff in Virginia complained about the lack of information from the FBI pertaining to his county. He stated that the information he received was no different than what he saw in the media. However, although this Sheriff assigned one of his deputies as a liaison to the local JTTF, neither the Sheriff nor the liaison possess, or had applied for, Secret or Top Secret clearance. When asked why not, the Sheriff stated that he believed having to apply for and obtain a security clearance to receive information from the FBI was an insult to a veteran law enforcement official.*[94]

Other observers have raised additional concerns about the limited utility of security clearances for information sharing purposes. "The federal government should work to declassify as much information as possible instead of requiring security clearances for intelligence consumers," the Heritage Foundation noted.[95] "Forcing states and localities to incur the costs of the security clearance process is an undue burden since these entities are helping the federal government to protect the nation."[96] CRS, in turn,

---

[93] Carter, supra note 10, Chapter 11: Federal Law Enforcement Intelligence 164, available at http://www.cops.usdoj.gov/default.asp?Item=1404.

[94] United States Department of Justice, Office of the Inspector General, Evaluation and Inspections Division, The Department of Justice's Terrorism Task Forces 33 n.19 (June 2005) [hereinafter "The Department of Justice's Terrorism Task Forces"].

[95] James Jay Carafano, Paul Rosenzweig, and Alane Kochems, "An Agenda for Increasing State and Local Government Efforts to Combat Terrorism," Heritage Foundation (Feb. 24, 2005), at http://www.heritage.org/Research/HomelandDefense/bg1826.cfm.

[96] Id.

estimated the cost of conducting required background checks at $2,500 apiece – paid for, in some cases, with discretionary federal homeland security grant funds.[97] CRS likewise questioned how state officials with Top Secret clearances would be able to use classified information to direct the actions of other uncleared state personnel, and how the integrity of classified information would be maintained in terms of detecting and addressing security breaches.[98] Furthermore, it is far from certain that a security clearance granted by one intelligence agency will be recognized and honored by another intelligence agency. As Joe Polisar, Chief of the Garden Grove, California, Police Department recently commented:

> *As an appointee to the Homeland Security Science and Technology Advisory Committee, I went through a nine-month process to obtain a Department of Homeland Security Top Secret Security Clearance. Once I received it, however, I discovered that the FBI could not immediately recognize it for information sharing purposes. Specifically, until my DHS Top Secret clearance was recognized by the FBI, any top secret information that the FBI had supplied to one of my officers assigned to our local Joint Terrorism Task Force could be held from me. Because I held a DHS Top Secret Clearance and the officer held an FBI Top Secret Clearance, I was forced to submit my information to the FBI through the DHS and had to wait eight months before the Bureau recognized my DHS Top Secret clearance. If there had been any terrorist activity in my jurisdiction in the meantime, I might have been shut out of the loop. This obviously is not an optimal solution. If the feds are having this kind of difficulty recognizing each other's clearances, how are we in law enforcement ever going to be full players in the country's homeland security efforts?*[99]

The Department's Homeland Security Advisory Council (HSAC), a group that includes numerous state, local, tribal law enforcement officers as well as other first responders, has concluded that providing security clearances to every officer across the nation is not the best approach. "The Federal Government should emphasize providing current and actionable and unclassified information," the HSAC noted in its December 2004 report.[100] "The emphasis should not be on providing security clearances and forcing related security costs on state and local government officials."[101] Rather than expanding the legal definition of the IC to include state, local, and tribal entities, the

---

[97] See Relyea and Siefert, supra note 36 at CRS 22.

[98] Id. See also Police Executive Research Forum, Protecting Your Community from Terrorism: Strategies for Local Law Enforcement 21 (March 2003) ("Local members on JTTFs also cannot always debrief their own commanders because of the security clearance restrictions . . ."), at http://www.cops.usdoj.gov/mime/open.pdf?Item=1364.

[99] Telephone Interview with Joseph Polisar, Chief of Police, Garden Grove, California Police Department (Nov. 22, 2005).

[100] Department of Homeland Security Homeland Security Advisory Council, Intelligence and Information Sharing Initiative Final Report – December 2004 2 (2004), available at http://www.dhs.gov/interweb/assetlibrary/HSAC_ExecSummIntelInfoSharingReport1_1204.pdf.

[101] Id.

HSAC continued, "[t]he emphasis should be on establishing the processes, protocols and systems to facilitate the sharing of intelligence/information between those who collect it and those who need it."[102] The HSAC further recommended that the federal government develop a single pipeline that integrates intelligence information from multiple sources, and that delivers intelligence information rapidly, concisely and in an actionable (i.e., unclassified) format that can be updated regularly.[103]

Nondisclosure Agreements

The Homeland Security Act likewise suggested that nondisclosure agreements might be an effective means for promoting the sharing of "sensitive but unclassified" information with state, local, and tribal law enforcement officers.[104] Taking this cue, the Department promulgated a management directive and prepared a companion Non-Disclosure Agreement (NDA) for this purpose.[105] The directive – since amended – initially required all employees to sign an oath that they would not disclose such information without proper authorization.[106] It likewise treated "sensitive but unclassified information" and "For Official Use Only" (FOUO) information as one in the same, defining them as "unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest . . .FOUO is not to be considered classified information."[107]

Observers quickly concluded that requiring people to execute NDAs to protect unclassified information made little sense in most cases, describing the Department's initial directive as both "unprecedented"[108] and "extraordinary" [109] and noting that "no

---

[102] Id., Powerpoint Presentation at 24 (emphasis in original), available at http://www.dhs.gov/interweb/assetlibrary/HSAC_IntelInfoSharingReport_1204.pdf.
[103] Id., Powerpoint Presentation at 21.
[104] Homeland Security Act, §§ 892(c)(2)(B). As a point of clarification, the nondisclosure agreements referred to in this section were intended to address sensitive but *unclassified* information. They are different from the Standard Form 312 Classified Information Nondisclosure Agreement that all people who obtain security clearances must sign before being provided access to classified information.
[105] Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD Number: 11042 at http://www.fas.org/sgp/othergov/dhs-sbu.html, superseded by Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD Number: 11042.1 at http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf; Department of Homeland Security Non-Disclosure Agreement, DHS Form 11000-6 (08-04) at http://www.fas.org/sgp/othergov/dhs-nda.pdf.
[106] Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD Number: 11042 at http://www.fas.org/sgp/othergov/dhs-sbu.html.
[107] Id.
[108] Eileen Sullivan, "Searches and Gag Orders: Homeland Security's Unprecedented Campaign Cloaks Unclassified Information," FederalTimes.com, (Dec. 6, 2004) at http://federaltimes.com/index.php?S=537895.

other executive branch agency systematically requires a non-disclosure agreement for access to unclassified FOUO [for official use only] information."[110] The presidents of two labor unions representing Department employees consequently asserted that while employees "'fully appreciate' the need to safeguard classified and other highly-sensitive information . . . the DHS directive covers 'a virtually unlimited universe of information that is relevant to important matters of public concern' and whose disclosure would have no adverse impact on the national security."[111] Accordingly, the union presidents wrote, "the directive and the accompanying non-disclosure agreement employees are being made to sign 'actually undermine our national security and the public interest.'"[112] The anticipated impact of NDAs on information sharing efforts was expected to be negative:

> *Some government secrecy experts, such as Bill Leonard, director of the Information Security Oversight Office at the National Archives and Records Administration, said they fear the department's policy will squelch information sharing among the department, the public and other federal, state and local organizations. "It creates an environment exactly opposite, I think, what we're trying to do in the name of information sharing," Leonard said. "It creates an environment of uncertainty. And in an environment of uncertainty, most people resort to a default position of 'Do not share, because otherwise I might inadvertently violate a rule or regulation or a regime that I'm not even familiar with.'"*[113]

Given these difficulties, the Department rescinded the requirement that employees sign NDAs as a condition of employment, describing them as an "interim measure" that would be superseded by an education program designed to teach employees how to protect sensitive but unclassified information.[114] A new Department directive issued earlier this year, however, continues to require contractors and consultants to sign NDAs.[115] Growing concern about the relatively amorphous definition of "sensitive but unclassified" information, however, has prompted legislation that could lead to the elimination of this classification designation altogether – a development that would render even the current contractor and consultant NDAs obsolete.[116]

---

[109] Federation of American Scientists, "Department of Homeland Security Tightens Grip on Unclassified Info," Secrecy News, Vol. 2004, Issue No. 53 (June 11, 2004) at http://www.fas.org/sgp/news/secrecy/2004/06/061104.html.
[110] Id.
[111] Press Release, National Treasury Employees Union and American Federation of Government Employees, NTEU, AFGE Protest DHS Action Expanding Management Ability to Suppress Information (Nov. 29, 2004) (on file with author).
[112] Id.
[113] Sullivan, supra note 108.
[114] Audrey Hudson, "Agency Drops Nondisclosure Rule for Workers," Washington Times (Jan. 18, 2005) available at http://www.washingtontimes.com/functions/print.php?StoryID=20050117-113208-2946r.
[115] Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD Number: 11042.1 at http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf.
[116] The Restore Open Government Act, H.R. 2331, 109th Cong. (2005); see also James J. Carafano & David Heyman, DHS 2.0: Rethinking the Department of Homeland Security, the Heritage Foundation and the Center for Strategic and International Studies, at http://www.csis.org.hs/041213_dhsv2.pdf (Dec. 13, 2004),

While the Department actively pursued NDAs internally, it initiated no coordinated, parallel effort to have state, local, or tribal law enforcement officers sign such agreements. On the contrary, obtaining executed NDAs from such people was typically a belated, sporadic affair. "To support the dissemination of time-critical threat information, on occasion, those in receipt of such information were asked, after the fact, to sign a NDA," one former Department official stated.[117] "The current Department NDA policy is not being implemented in any cohesive manner that is either constructive to the Department or useful to those that require receipt of Department information."[118] Addressing what steps the Department might be taking to correct this deficiency, the official added, "To my knowledge, there is not an effort underway to encourage state and local officials nor private sector leaders to sign these NDAs thus allowing the Department to maintain a record of who is cleared and accountable for receipt of sensitive information."[119] This situation reflects the conclusion by at least some Department personnel that executing a NDA amounts to little more than an administrative burden that does not advance the cause of information sharing. "An NDA isn't necessarily something that automatically engenders the trust that is needed to cause people to share," said Sue Reingold, Associate Director of the Department's Office of State and Local Government Coordination.[120] "It's a complicated business that requires a better federal-state-local-private sector partnership to identify the most effective mechanisms for sharing and the best way to get rid of barriers."[121]

Joint Terrorism Task Forces, Anti-Terrorism Advisory Councils, and Terrorism Early Warning Groups

In addition to security clearances and NDAs, the Homeland Security Act also proposed an "increased use of information-sharing partnerships" as a third option for providing police and sheriffs' officers with the law enforcement intelligence they need.[122] The Department of Justice's JTTFs, for example, are squads within the FBI's field offices that focus on addressing terrorism threats and preventing terrorist incidents.[123] The JTTFs, "tackle a wide array of potential terrorist threats and conduct investigations related to terrorist activities within the geographic region where the particular JTTF is headquartered."[124] By pooling the resources of multiple agencies, and by drawing on the expertise of not only federal but also state, local, and tribal law enforcement officers

---

at 20 (citing increasing secrecy within the federal government involving sensitive but unclassified information – as well as abuses by various agencies – and noting, "At the very least, such wholesale withdrawal of information seems arbitrary and undermines important values of government openness, the development of electronic government (e-gov) to speed the delivery and lower the cost of government services, and public trust.").

[117] Telephone Interview with Department Official (Aug. 31, 2005) (notes on file with author).

[118] Id.

[119] Id.

[120] Telephone Interview with Sue Reingold, Associate Director, Office of State and Local Government Coordination, Department of Homeland Security, in Washington, D.C. (Aug. 18, 2005).

[121] Id.

[122] Homeland Security Act, §§ 892(c)(2)(C).

[123] The Department of Justice's Terrorism Task Forces, supra note 94 at 16.

[124] Carter, supra note 10 at 170.

assigned to their ranks, JTTFs are able to collect and share classified and unclassified information with their partners at all levels of government.[125] As FBI Director Robert S. Mueller III has noted, "JTTFs team up FBI agents with police officers, members of the Intelligence Community, Homeland Security, and other federal partners to coordinate counterterrorism investigations and share information. They are also a critical conduit between the FBI and the officer on the beat."[126] JTTFs not only help the FBI share information with state and local police agencies but also contribute to enhanced government efforts to protect the nation.[127] There are presently 103 JTTFs throughout the United States.[128] Prior to the 9/11 attacks, there were 912 JTTF members nationwide.[129] By January 2005, that number had jumped to 5,085 members.[130]

The Department of Justice's Anti-Terrorism Advisory Councils (ATACs) – formerly ATTFs – complement the JTTF effort by working to both coordinate the dissemination of terrorism information and develop investigative and prosecutorial strategies in each United States Attorneys' Office across the nation.[131] Established by the Attorney General in the wake of 9/11, ATACs "provide a central forum for agencies to congregate and identify potential terrorism links among their investigations. As the entities that work regularly with all enforcement agencies, [ATACs] are positioned to bring agencies together which would not otherwise know that their respective investigations are linked."[132] ATACs have a threefold objective: preventing, disrupting, and defeating terrorist operations before they occur; developing and implementing the full range of resources available to investigate terrorist incidents and bring their perpetrators to justice; and vigorously prosecuting those who have committed, or intend to commit, terrorist acts in the United States."[133] They accordingly have three principal functions: coordinating anti-terrorism initiatives and providing organized structure to respond to terrorist incidents; sponsoring training to neutralize suspected terrorists and terrorist supports; and facilitating information sharing between federal and local agencies on terrorism-related matters.[134]

While the work of the JTTFs and ATACs is critical, the information they share is not necessarily the type of information that will help state, local, or tribal law

---

[125] Id.
[126] U.S. Congress. Senate. Select Committee on Intelligence. Closed Hearing on Intelligence Matters. 108th Cong., 2nd sess., 2004 (prepared statement of Robert S. Mueller, III, Director, FBI), available at http://www.fbi.gov/congress/congress04/mueller022404.htm.
[127] Mefford, L. (June 12, 2003). "Inside the FBI: FBI's Counterterrorism Unit," Washingtonpost.com: Larry Mefford Weblog, available at http://discuss.washingtonpost.com/zforum/03/r_nation_fbi061203.htm.
[128] The Department of Justice's Terrorism Task Forces, supra note 94 at 16.
[129] Id. at 18.
[130] Id.
[131] The Department of Justice's Terrorism Task Forces, supra note 94 at 11-12.
[132] See Memorandum from the Attorney General to all United States Attorneys (Sept. 24, 2003), available at http://usanet.usa.doj.gov/site_index/pdf_memos/atac.pdf.
[133] U.S. Government Accounting Office, U.S. Attorneys: Performance-Based Initiatives Are Evolving, GAO-04-422, (Washington, D.C.: GAO, May 2004), 56 n.4.
[134] National Native American Law Enforcement Association, Tribal Homeland Security Forum Report 27 (July 2004), available at http://www.nnalea.org/hlsecurity/NNALEAForumFinal-Final.pdf.

enforcement officers detect and thwart terrorist attacks. On the contrary, it is important to distinguish between (1) "investigative" intelligence – the type of information that pertains to ongoing investigations or that requires investigative action; and (2) "preventative" intelligence – the type of information that can be used to inform front line law enforcement about what threats they need to address in their communities by making sense of the information that they themselves develop as part of their day-to-day policing activities.[135] Although both forms of intelligence seek to prevent terrorist attacks, investigative intelligence "is designed to punish those who commit terrorist attacks and seeks evidence that is legally admissible in court," noted Lee H. Hamilton, former Vice Chair of the 9/11 Commission.[136] Preventative intelligence, on the other hand, "is designed to prevent terrorist attacks before the fact, and seeks information to thwart planned attacks, regardless of whether it is legally admissible."[137]

Assistant United States Attorney Thomas C. Taylor has observed that JTTFs and ATACs have traditionally generated investigative intelligence with criminal prosecutions at the heart of their work.[138] Addressing the role of the Intelligence Research Specialist (IRS) within each United States Attorneys' Office, Taylor stated:

> *The IRS provides the U.S. Attorney with access to classified criminal intelligence, as well as unclassified "Law Enforcement Sensitive" intelligence. He or she coordinates intelligence activities with and between the members of a district's Anti-Terrorism Advisory Council (ATAC) (formerly the Anti-Terrorism Task Force) and the Joint Terrorism Task Force (JTTF). The goal of this intelligence information is to share information and resources needed to detect terrorist networks and to arrest and prosecute terrorists before they act.*
>
> * * *
>
> *The Attorney General stated that ATACs "provide a central forum for agencies to congregate and identify potential terrorism links among their investigations. As the entities that work regularly with all enforcement agencies, [ATACs] are positioned to bring agencies together which would not otherwise know that their respective investigations are linked."*[139]

---

[135] Weston Aug. 19 Email, supra note 8 (asserting that intelligence reports dealing with ongoing investigations or intelligence requiring investigative action should remain within the purview of JTTFs and intelligence of a preventative nature should be addressed by a separate entity with access to IC information resources).

[136] U.S. Congress. Senate. Committee on the Judiciary. FBI Oversight. 109th Cong., 1st sess., 2005 (prepared statement of Lee H. Hamilton, former Vice Chair of the 9/11 Commission) [hereinafter Hamilton FBI Oversight Statement], available at http://www.9-11pdp.org/press/2005-07-27_testimony.pdf.

[137] Id.

[138] Thomas C. Taylor, "An Overview of the Intelligence Research Specialist Program," First Responders 3 (July 2004), at http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5204.pdf.

[139] Id. (emphasis added).

While ATACs play a primarily organizational role in the sharing of this type of information, Taylor added, "[t]he JTTF is largely operational, dealing with intelligence collection, analysis, and investigation."[140] A JTTF accordingly uses "all investigative and prosecutorial tools at its legal disposal (laws related to illegal firearms, financing, narcotics, etc.) . . . for the express purpose of stopping acts of terrorism within the U.S."[141]

Unlike investigative intelligence, preventative intelligence is not constrained by probable cause and other legal concerns because it is not gathered for use in a criminal case.[142] Accordingly, it encompasses information that – although not legally admissible at a trial – might still inform law enforcement efforts about what operations to undertake, who and what to protect, and when to harden potential terrorist targets against attack.[143] Preventative intelligence requires "significantly greater investment, most noticeably in terms of skilled personnel who are capable of interpreting material and deciding which of many warnings received each day represent a real and credible threat."[144] Given the FBI's traditional law enforcement focus, many have doubted its ability to make this investment:

> *Skeptics assert that the FBI's entrenched law enforcement culture will undermine its efforts to establish an effective and efficient intelligence program by centralizing decision-making at FBI headquarters. They point to the historical importance that the FBI has placed on convicting criminals – including terrorists. But those convictions have come after the fact, and skeptics argue that the FBI will continue to encounter opposition within its ranks to adopting more subtle and somewhat unfamiliar intelligence methods designed to prevent terrorism. Former Attorney General Janet Reno, for example, reportedly "leaned toward closing down surveillance under the Foreign Intelligence Surveillance Act (FISA) if they hindered criminal cases." As one observer said, "law enforcement and intelligence don't fit . . . law enforcement always wins."*[145]

The Gilmore Commission concurred, concluding, "[T]he Bureau's long-standing traditional organizational culture persuades us that, even with the best of intentions, the FBI cannot soon be made over into an organization dedicated to detecting and preventing

---

[140] Id. at 4.
[141] Blair C. Alexander, Strategies to Integrate America's Local Police Agencies Into Domestic Counterterrorism (U.S. Army War College: Carlisle Barracks, Pennsylvania), March 18, 2005, available at http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil178.pdf.
[142] Hamilton FBI Oversight Statement, supra note 136.
[143] Id.; see Weston Aug. 19 Email, supra note 8.
[144] "Where Does US Intelligence Go From Here – And Were They Really to Blame?" Jane's Intelligence Digest, Sept. 27, 2001, available at http://www.janes.com/security/international_security/news/jid/jid270901_1_n.shtml.
[145] Alfred Cumming and Todd Masse, FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress, **Congressional Research Service**, Aug. 4, 2004, CRS 18 (citations omitted), available at http://hutchison.senate.gov/RL32336.pdf.

attacks rather than one dedicated to punishing them."[146] The FBI in fact has met with decidedly mixed results in generating preventative intelligence:

> *With respect to the case-orientation and law enforcement bias so often mentioned as challenges for the FBI as it shifts to having a more preventative bias, state and local law enforcement officials stated that notwithstanding recognition by FBI leadership that the "intelligence is in the case," the FBI agent on the street still starts with a case and has a bias in the direction of law enforcement. Moreover, one senior state law enforcement official stated that FBI leadership is ". . . still being led by individuals who have a criminal law mindset."*[147]

Given their traditional law enforcement focus and accordant close relationship with the FBI, neither JTTFs nor ATACs appear to be optimal vehicles for generating and conveying preventative intelligence to state, local, and tribal law enforcement at this time. Even if they possessed robust capacities in this regard, however, other factors limit JTTF and ATAC utility for information sharing purposes.

Perhaps the greatest obstacle to effective JTTF information sharing is the fact that much of the information that JTTFs possess is classified – a situation that obliges police and sheriffs' officers assigned to their ranks to first obtain security clearances before accessing that information.[148] As discussed previously, if an officer assigned to a JTTF cannot share what he or she knows with his or her colleagues who do not also have clearances, frustrations understandably mount. The City of Portland, Oregon, for example, recently pulled out of its local JTTF after the FBI refused to provide the mayor with a top secret clearance that he believed he needed in order to communicate with and otherwise oversee city police officers working with the JTTF.[149] One local law enforcement officer likewise complained that at his JTTF, "the sharing has a lot of room for improvement," noting that friction between local police and the FBI in his jurisdiction is "legendary."[150]

---

[146] **Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Fourth Annual Report to the President and Congress** 43-44 (Dec. 15, 2002), available at http://www.rand.org/nsrd/terrpanel/terror4.pdf.

[147] Cumming and Masse, supra note 145 at CRS 34 (citations omitted).

[148] U.S. Congress. House. Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Governments. 108th Cong., 2nd sess., 2004 (prepared statement of Willie T. Hulon, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation), available at http://www.fbi.gov/congress/congress04/bald071304.htm.

[149] "County Takes Portland's Spot on Terrorism Task Force," The Oregonian (June 29, 2005), available at http://www.lexis.com/research/retrieve/frames?_m=13f0f8100e52b204f72932c225cf1b3a&csvc=bl&cform=bool&_fmtstr=XCITE&docnum=1&_startdoc=1&wchp=dGLbVlz-zSkAW&_md5=cf65f0d7663c8fc8d0812331b03e1172.

[150] Justin Rood, "Pentagon Has Access to Local Police Intelligence Through Office in Homeland Security Department, CQ.com, July 6, 2004, available at http://www.cq.com/corp/show.do?page=temp/20040708_homeland.

Moreover, while the DOJ OIG recently concluded that JTTFs and ATACs have "generally functioned as intended, without significant duplication of effort, and they contribute to the Department's goal to prevent terrorism and promote national security,"[151] it warned that they have not coordinated their information sharing efforts in so-called "remote" areas:

> *Although the FBI and ATACs have ongoing efforts to interact and share information with law enforcement agencies and first responders in remote areas, some ATACs and JTTFs have not used all their resources to reach remote agencies that do not have representatives on the task forces and councils. The state and local law enforcement agencies with members on a JTTF or ATAC were satisfied with the amount and type of terrorism information shared. In contrast, those law enforcement agencies that were outside of the metropolitan areas and that did not have task force or council members were not as satisfied. Most remote law enforcement agencies often do not have the resources of the distance is too far to commit representatives to a JTTF and ATAC, but they still need information on terrorism from the federal government as well as terrorism-related training. The JTTFs and ATACs do not have coordinated strategies with each other to address the gaps in information sharing and training. Because terrorism and the terrorism threat may be found throughout the country, remote areas cannot be overlooked.*[152]

These gaps are particularly disturbing because DOJ OIG defined a "remote" area as "an urban or rural area outside the vicinity of the physical location of the ATAC and JTTF."[153] Because many JTTFs and ATACs are responsible for providing coverage for entire states or even across multiple states,[154] most of the country could be considered "remote" – leaving vast areas either "unserved" or underserved by these entities. This gap could be devastating. "The nature of terrorism is to flow around obstacles and find the path of least resistance," noted Charles V. Pena, the Director of Defense Policy Studies at the CATO Institute.[155] Given the limited presence of both JTTFs and ATACs, it seems likely that terrorists will move their operations beyond their reach in order to avoid detection.

In addition to JTTFs and ATACs, Congress also suggested TEWs as potentially effective information sharing models.[156] TEWs had their genesis within the Los Angeles County Sheriff's Department during the summer of 1996 following a series of major terrorist incidents around the world that culminated in Osama bin Laden's call for attacks

---

[151] The Department of Justice's Terrorism Task Forces, supra note 94 at Executive Digest, ii.
[152] Id. at v.
[153] Id. at 84 n. 48.
[154] Id. at 84.
[155] Charles V. Pena, "Homeland Security: Follow the Bouncing Ball," CATO Institute (May 6, 2003), available at http://www.cato.org/dailys/05-06-03.html.
[156] Homeland Security Act, §§ 892(c)(2)(C).

on the United States and its interests.[157] The Sheriff's Department established the TEW in order "to form a countywide group that was capable of a highly coordinated and focused response to acts of terrorism, based on careful assessment of information and intelligence and detailed planning."[158] The TEW: (1) monitors trends and assesses threats that could result in terrorist attacks; (2) establishes protocols to identify and distinguish those threats credible enough to warrant a response and determine the level of response required; and (3) assesses threats or hoaxes, suspicious devices, and outbreaks of disease.[159] Among other things, the TEW maintains "intelligence reservoirs" that are updated to provide a clear picture of likely terrorist incidents.[160] As part of its advance planning work, the TEW develops detailed scenarios to respond to those incidents and which take into account the different levels of response that might be required.[161] "The most obvious use of this information is to guide the response to an attack," an observer noted, "but the information can also highlight ways to make targets less vulnerable in the first place. And the unit's [TEW's] highest goal is to spot the signs of an impending attack in time to stop it altogether." [162] The TEW also provides training and exercises to improve and maintain the skills of its partners.[163] In Los Angeles County, those partners include the Sheriff's Department, the Los Angeles Police Department, three public health services, the FBI, the Department, and approximately thirty (30) additional agencies – including emergency management services, fire departments, transportation authorities, universities, and airports.[164] Describing this arrangement, Los Angeles County Sheriff Leroy Baca noted:

> *This interagency approach allows for early response and enforcement by clearing the communication channels between agencies and creating an environment that facilitates information and intelligence sharing. The result is an effective network that has the ability to identify information which might indicate impending terrorist activity. This group is a significant resource for identifying and assessing potential threats, making appropriate notifications and recommendations, and aiding in mission planning and the efficient allocation of resources.*[165]

---

[157] Greg Krikorian, "Terrorism Early Warning Group Works to Keep L.A.'s Guard Up," Los Angeles Times, Nov. 8, 2004, available at http://www.policeone.com/policeone/frontend/parser.cfm?object=News&tmpl=&operation=full_news&id=93416.

[158] Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Terrorism Early Warning Group: Intelligence Coordination Among Federal, State, and Local Entities 1 (2005), available at http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf (hereinafter "TEW Brochure").

[159] Id. at 1-2.

[160] Id. at 2.

[161] Id.

[162] Sydney J. Freedberg Jr., "National Security: Homeland Improvement," National Journal, Sept. 13, 2002, available at http://pscommllc.com/news/nj_homeland_improvement.html.

[163] TEW Brochure, supra note 158 at 1.

[164] Id.

[165] Leroy D. Baca, "A Regional Response to Terrorism," Anti-Defamation League Law Enforcement Agency Resource Network (January 2003), available at http://www.adl.org/learn/columns/Leroy_D_Baca.asp?LEARN_Cat=Resources&LEARN_SubCat=OTB.

TEWs, however, are not in the business of traditional intelligence investigations, collection, or analysis. Although TEW directors and key members of their staffs typically have security clearances,[166] TEWs instead rely upon their FBI partners for access to classified material that the FBI sanitizes for TEW consumption.[167] The Orange County, California TEW, for example, maintains liaison officers within the FBI through the local JTTF.[168] "Having those in-house G-men enables TEW to act as a conduit for carefully declassified federal data," stated one commentator.[169] TEWS instead use open source information for the bulk of their information needs:

> *As important as the FBI's contribution is, however, the most important thing about the Terrorism Early Warning group is that it does not depend upon the federal government. Of necessity, TEW teams spend a lot of time on "open-source intelligence": painstakingly sifting news stories, official reports, and other public document to accumulate clues to what might be happening in secret (an approach federal spy agencies traditionally disdain). The group also reaches out to an ever-growing roster of expert contacts and consultants. And its member agencies can put their own investigators on the street.*[170]

The TEW takes this "blend of information . . . and puts together 'target folders' on specific vulnerable sites, and develops broader 'playbooks' for general types of threats, which outline weak points, attack scenarios, and potential responses."[171] In short, a TEW's job is to "analyze and disseminate that information in a way that will help in the terrorism fight."[172] When an attack does occur, a TEW disseminates information to the commanders in the field handling the response.[173]

---

[166] Krikorian, supra note 157 (noting that John P. Sullivan, the director of the Los Angeles County TEW and several of his close associates have security clearances that allow them to receive CIA reports and other classified material).

[167] Freedberg, supra note 162.

[168] U.S. Congress. House. Select Committee on Homeland Security. First Responders; How States, Localities and the Federal Government are Working Together to Make America Safer. 108th Cong., 1st sess., 2003 (statement of George Jaramillo, Assistant Sheriff, Orange County, California Sheriff's Department), available at http://fr.webgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_senate_hearings&docid=f:96816.wais.pdf.

[169] Freedberg, supra note 162.

[170] Id.

[171] Id.

[172] "Fighting Terror Here," Contra Costa Times, July 29, 2005, available at http://www.contracostatimes.com/mld/cctimes/news/editorial/12224418.htm?template=contentModules/printstory.jsp.

[173] TEW Brochure, supra note 158 at 3. The TEW model has been adopted not only in Los Angeles and Orange Counties in California but also in other regions – most recently in Kansas City, Missouri. E-mail from Ed Reed, Program Manager, TEW Expansion Project, Terrorism Research Center, Inc., to Meghan McPherson, Intern, House Committee on Homeland Security, Democratic Staff (Oct. 12, 2005, 15:59:00 EST) (on file with author). Plans for a TEW in Miami, Florida are also underway. Id. The Department's Office of State and Local Government Coordination and Preparedness is now using Urban Areas Security Initiative (UASI) grants to replicate TEW programs across the country. TEW Brochure at 4.

Although TEWs are excellent conduits of sanitized intelligence from the FBI, the extent to which their needs are actually driving that information flow is unclear. Participants at a recent seminar sponsored by the National Homeland Security Consortium in Monterey, California, noted that filtering information through a "hierarchal system" – specifically, the FBI – "is a significant impediment to the doctrine that information, to be useful, must be shared."[174] Consequently, while TEWs cooperate with the FBI and JTTFs to inform their security efforts, the fact that they rely upon open source information and other resources for many of their threat assessments and response strategies speaks volumes.

* * *

The ideas that Congress included in the Homeland Security Act to promote information sharing were just that – ideas. In practice, none of them offer a completely satisfactory resolution to the problem at hand: providing specific and actionable law enforcement intelligence to state, local, and tribal officers that informs their ability to thwart terrorists and their plans. Even if all these mechanisms worked seamlessly, however, they still would have to overcome the cultural barriers to sharing law enforcement intelligence that continue to plague the IC.

The "Need to Share" Meets The Intelligence Culture: A Major Information Sharing Obstacle

In order to spur greater information sharing of law enforcement intelligence between the federal government and state, local, and tribal authorities, many commentators have emphasized that the IC must replace its Cold War "need to know" mentality with a "need to share" approach.[175] The Markle Foundation, one of the original proponents of this model, reasons that if agents and analysts at the outset of their work prepared intelligence products with an eye toward distributing them to as many appropriate people as possible (preferably, at an unclassified level), then pushing information to first responders would be a far easier, efficient, and consequently more effective affair.[176] The Department's HSAC agrees, noting that effective intelligence/information fusion requires, among other things, "[u]nderstanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide

[174] National Homeland Security Consortium, Homeland Security Executive Education Seminar, Summary Document 6 (May 24, 2005), available at http://www.nemaweb.org/?1392.
[175] U.S. Congress. House. Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations. Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing. 108th Cong., 2nd sess., 2004 (prepared statement of Bill Crowell, Markle Taskforce on National Security in the Information Age), available at http://www.markle.org/downloadable_assets/bill_crowell_testimony.pdf.
[176] **Markle Foundation Second Report** 23.

and/or local fusion efforts) . . . "[177] The HSAC adds that, "Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about who the enemies are, where and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use."[178] The challenge of consistently converting law enforcement intelligence from a classified to an unclassified or "less classified" format in a way that is responsive to these needs, however, remains a difficult problem.

As even the President acknowledges, most law enforcement intelligence could be declassified and disseminated to the state, local, and tribal levels simply by removing sensitive source and method information from relevant documents – information that most officers themselves generally do not want.[179] "Chiefs and sheriffs agreed they need to know that a source is credible and reliable when receiving information," one police observer noted.[180] "They do not always need to know the individual or specifics of how the information was obtained."[181] Less than a year after the 9/11 attacks, John Cary Bittick, the former President of the National Sheriff's Association, concurred with this assessment:

> *I am confident in stating that county sheriffs do not want access to sources and methods of intelligence gathering. We are unconcerned whether the information came from satellite intelligence, interviews with a foreign national or through electronic intercepts. However, sheriffs are extremely concerned with the timing and location of a potential attack, the method of attack, and other details that would enable us to prevent and prepare for an attack.*[182]

Added one JTTF observer, "[T]he threat usually can be discussed [with appropriate law enforcement officials] even if a sensitive source or method of how the threat was received cannot."[183] Former FBI Director William H. Webster accordingly has emphasized that

---

[177] Department of Homeland Security, Homeland Security Advisory Council, Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion 4 (April 28, 2005), available at http://www.dhs.gov/interweb/assetlibrary/HSAC_HSIntelInfoFusion_Apr05.pdf. The HSAC has described intelligence/information fusion as the "overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private-sector authorities." Id. at 3.

[178] Id. at 2.

[179] Critical Infrastructures Strategy, supra note 21.

[180] Gerard R. Murphy, et al., Police Executive Research Forum and United States Department of Justice Office of Community Oriented Policing Services, Protecting Your Community from Terrorism" The Strategies for Local Law Enforcement Series; Volume 1 – Improving Local-Federal Partnerships 23 (March 2003), available at http://www.mipt.org/pdf/Protecting-Your-Community-From-Terrorism.pdf.

[181] Id.

[182] U.S. Congress. House. Committee on the Judiciary, Subcommittee on Crime. Hearing on the Homeland Security Information Sharing Act. 107th Cong., 2nd sess., 2002 (statement of John Cary Bittick, then President of the National Sheriff's Association), available at http://judiciary.house.gov/legacy/bittick060402.htm.

[183] James Casey, "Managing Joint Terrorism Task Force Resources," FBI Law Enforcement Bulletin (Nov. 2004), available at http://www.au.af.mil/au/awc/awcgate/fbi/joint_terrorism_tf.pdf.

sources and methods "must be protected and honored if law enforcement and intelligence agencies are to be effective in recruiting and utilizing information obtained at great risk from such sources."[184] He therefore believes it is appropriate to supply first responders with what he calls "finished intelligence" that sets forth specific and actionable information without disclosing these sensitive details.[185] There are two approaches to sanitizing an intelligence report to reach this "finished" state:

> *One way is to use a "tear line" report in which an intelligence report has a segment, perhaps at the bottom of the page, where critical information is summarized and sources and methods are excluded. This portion of the report may be "torn off" (at least figuratively) and shared with persons who have a need to know the information but do not have a security clearance. The second method is to write intelligence products in a way that relays all critical information but excludes data that should remain classified.*[186]

Markle Foundation President Zoe Baird has been a long-time proponent of both methods. In congressional testimony last year, she described her organization's Systemwide Homeland Analysis and Resource Exchange (SHARE) Network, noting that it is based on the concept of "write to share."[187] "By taking steps like incorporating 'tear lines' in document formats," Baird explained, "SHARE would encourage reports that contain the maximum possible amount of sharable information."[188] More recently, she observed that the tearline approach makes intelligence easier to disseminate, stating that a tearline report "could include a paragraph explaining sourcing, and then a line drawn under that paragraph, separating information on sourcing from the information itself; the contents below the tear line could be shared with lower classification levels."[189] Baird has likewise touted the rapidity with which intelligence information parsed in this fashion could be disseminated to state, local, and tribal law enforcement officers. "[T]technology can be used to electronically separate the classified portions of a report ("above the tear line") from those that are unclassified ("below the tear line")," she explained.[190] It also can be used to "scrub data" such that classified information – such as a source's name – can be removed from a report before it is distributed.[191] William Crowell, a security consultant with extensive information sharing policy experience and a member of the Markle Foundation Task Force on National Security in the Information Age, has

---

[184] U.S. Congress. Senate. Committee on the Judiciary. FBI Oversight. 109th Cong., 1st sess., 2005 (statement of former FBI Director William H. Webster) (on file with author).
[185] Id. at 5.
[186] Carter, supra note 10; Chapter 11: Federal Law Enforcement Intelligence 165.
[187] U.S. Congress. House. Select Committee on Homeland Security. Hearing on Information Sharing After September 11: Perspectives on the Future. 108th Cong., 2nd sess., 2004 (statement of Zoe Baird, President, Markle Foundation, Chairman, Task Force on National Security in the Information Age), available at http://www.markle.org/downloadable_assets/zb_testimony_6.24.04.pdf.
[188] Id.
[189] Zoe Baird, Building Trusted Information-Sharing Environments for National Security and Health Care, Key Note Speech before the e-Gov Institute (June 1, 2005) (speech available at http://www.markle.org/downloadable_assets/baird.speech_060105.pdf).
[190] Id.
[191] Id.

emphasized that such tear lining would allow the IC to disseminate multiple versions of the same information to different audiences:

> *In our suggested approach, the production of such alternate versions would be commonplace and automatic. And it would be a top priority. For example, an agency would create a 'Top Secret/Code Word' report that reveals the source of the information; a 'Secret' version that would not reveal the source, but might give explicit detail on the threat; and a 'Sensitive But Unclassified' version that might only contain the necessary action the recipient agencies should take given their specific roles in the network (for example, to be on the lookout for certain individuals or indicators of specific terrorist activity).*[192]

The Markle Foundation's proposals have had a wide impact throughout the federal government – perhaps most notably in Executive Order 13356, which drew on SHARE extensively, as well as on the 9/11 Act itself, which encouraged the use of tearlines and essentially based the ISE on the SHARE model.[193] A number of intelligence agencies have also adopted key aspects of the SHARE approach. "The FBI, for example, has taken a number of positive steps in developing its new information sharing policies," Baird advised, "including adopting a potentially extremely important policy of 'writing for release,' which encourages tear lines and 'sharing[ing] by rule and withhold[ing] by exception.'"[194] More specifically, FBI Executive Assistant Director for Intelligence Maureen Baginski reported last summer that the FBI Office of Intelligence was developing a revised report-writing style that would facilitate information sharing immediately, including with those intelligence customers who did not have security clearances.[195] The NSA, moreover, has implemented its own "write-to-release" policy "to get information to customers at the lowest possible classification level and to facilitate the further sharing of that information with others who need it but are not directly supported by NSA."[196] The CIA likewise has followed a similar approach for years.[197] "At the end of each threat report," one former CIA employee noted, "an unclassified 'tear line' version of the intelligence is always included for passage to people without security clearances, like policemen or airline employees."[198]

Despite these steps, however, the greatest threat to "promising information and intelligence sharing initiatives" is neither a technical challenge nor a procedural

---

[192] See Crowell, supra note 175.
[193] Exec. Order No. 13,356, 69 Fed. Reg. 53599 (Aug. 27, 2004); 9/11 Act, § 1016.
[194] See Baird, supra note 187.
[195] See Carter, supra note 10, Chapter 3: A Brief History of Law Enforcement Intelligence: Past Practice and Recommendations for Change 34.
[196] United States Department of Defense, Report to Congress on the Role of the Department of Defense in Supporting Homeland Security 13 (Sept. 2003), available at http://biotech.law.lsu.edu/blaw/DOD/manual/.%5CFull%20text%20documents%5CAgencies%20Documents%5CDoD%20Role%20in%20HS%20-%201404.pdf.
[197] Thomas Patrick Carroll, "The 9/11 Commission Report: A Former CIA Officer's Perspective," Jamestown Foundation Terrorism Monitor (Sept. 2004), available at http://www.jamestown.org/publications_details.php?volume_id=400&issue_id=3080&article_id=2368574.
[198] Id.

obstacle.[199] Instead, it is "the cultural morass of institutional bias, federal-centric focus, and mutual misunderstanding that has too frequently inhibited law enforcement and intelligence communities."[200] Bert B. Tussing, Professor of National Security Affairs of the Center for Strategic Leadership at the U.S. Army War College, noted that the cultural hurdles to be overcome include, "ownership and control issues in the federal intelligence and law enforcement sectors; the 'federal-centric' focus in domestic intelligence operations; as well as building greater interdepartmental and intragovernmental understanding."[201] By most accounts, these cultural issues continue to plague the IC and its interactions with state, local, and tribal law enforcement authorities. "The rivalries among law enforcement agencies are acute because of competition for funds, overlapping authority, different cultures, the FBI's traditional hauteur, and fear of a rival agency's "stealing" one's cases," recounted Richard A. Posner, a judge with the United States Court of Appeals for the Seventh Circuit.[202] "Many local law enforcers feel deserted by the federal government in general, and the FBI in particular, in regard to national security intelligence. The Bureau does not treat them as its partners or even its customers."[203] Judge Posner, a longtime critic of the 9/11 Commission, speaks from personal experience, in stating that "FBI agents have been known to brush off attempts by local police, and even by other federal officers, to obtain the Bureau's aid in intelligence matters."[204] He added, "I am told that the FBI turned down an offer of a simple computer-communications system that would have linked the Joint Terrorism Task Forces directly to squad cars so that police officers could send and receive timely information concerning possible terrorist activities."[205] Changing these culturally ingrained behaviors is no easy task. "As much as federal agents may intellectually understand that information sharing in this new global threat scenario is good, it goes against everything they've always believed deep down in their guts," stated another commentator, "So a big, integrated system for sharing case information may make sense, but it probably feels to the G-men like a highway to hell."[206]

This unfortunate landscape has its roots in the historically different missions of federal intelligence agencies on the one hand and state, local, and tribal law enforcement authorities on the other. "Primarily intelligence officers collect information while law enforcement agents collect evidence," noted Ronald Marks, a Senior Fellow at the George Washington University Homeland Security Policy Institute (Institute) and a 16-year CIA veteran.[207] "This cultural difference affects the use and effectiveness of information. It is not going to change," he added, "Nor does America as a society want it

---

[199] Bert B. Tussing, Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process, and Culture, Center for Unconventional Security Affairs 12-13 (Jan. 2004), available at http://www.cusa.uci.edu/images/CUSAOP3Tussing.pdf.
[200] Id.
[201] Tussing, supra note 199.
[202] Richard A. Posner, Remaking Domestic Intelligence 58-59 (Hoover Press 2005).
[203] Id.
[204] Id.
[205] Id.
[206] Abbie Lundberg, "The Hard Road to Change," CIO Magazine, June 15, 2005, available at http://www.cio.com/archive/061505/edit.html?action=print.
[207] Ronald Marks, "Commentary: Defining America's Brave New World," Cambridge Review of International Affairs, Nov. 2, 2002, at 339.

to. While the gaps separating the two communities cannot be closed entirely, they can, and must, be bridged."[208] Frank J. Cilluffo, Associate Vice President of the Institute has expounded on this point, asserting that, "Law enforcement wants to string criminals up, whereas the IC wants to string them along. Intelligence agencies have been reticent to share information with law enforcement because of the desire to prevent discussion about their sources and methods in open court, a situation that would reveal this information to the world."[209]

There is no sign that these divisions will abate in the near term. As the authors of the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report (Robb-Silberman Report) recently noted:

> *[T]he Terrorist Threat Integration Center, now absorbed within the National Counterterrorism Center, has succeeded in establishing connections to dozens of networks at its new terrorism warning center – but obstacles remain. Representatives from one agency still face legal and policy barriers that prevent them from gaining access to the database of another. Collectors of information continue to operate as though they "own" the information, and collectors continue to control access to the information they generate. Decisions to withhold information are typically based on rules that are neither clearly defined nor consistently applied, with no system in place to hold collectors accountable for inappropriately withholding information.*[210]

Congressman Rob Simmons, Chairman of the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment concurred with this view during the Committee's July 2005 hearing on the Department's Second Stage Review.[211] "[W]ith a background in military intelligence and a period of time with the Central Intelligence Agency, I would say that information sharing goes completely against the culture of the intelligence community," he stated.[212] "If I go out and get myself a nice, juicy secret, I'm not about to share it with you or anybody else. I want to run it up the flagpole to my boss and get a kudos. So the whole idea of information sharing involves a cultural change in our intelligence community . . ."[213]

Daniel J. Prieto, a researcher affiliated with Harvard's Kennedy School of Government, noted earlier this year that turf battles and jockeying for position have

---

[208] Id.
[209] Frank J. Cilluffo, et al., "The Use and Limits of U.S. Intelligence," The Washington Quarterly, Winter 2002, at 71.
[210] Robb-Silberman Report, supra note 5 at 431.
[211] U.S. Congress. House. Committee on Homeland Security. Hearing on Review of Department of Homeland Security Organization. 109th Cong. 1st sess., 2005 [hereinafter Department of Homeland Security Organization Transcript] (Congressional Quarterly Transcript on file with author).
[212] Id.
[213] Id.

remained the only constant as federal intelligence agencies have undertaken much needed reforms in the post-9/11 environment – reforms that have not been helped by the DNI's own difficulties in establishing the authority of his office:

> *[C]ompetition within the intelligence community has risen as the FBI and Defense Department have opportunistically taken advantage of CIA blunders on Iraq intelligence to boost their own capabilities. The FBI has created a separate Intelligence Directorate. The Defense Department is creating a new spy division, the Strategic Support Branch, and Undersecretary of Defense for Intelligence Stephen Cambone is seeking to consolidate the Pentagon intelligence apparatus under his control to become a de-facto "mini DNI." With unclear authority and interagency rivalry as high as ever, the DNI's success is not a given, but will be determined by the outcome of his skirmishes with Mr. Mueller, CIA Director Peter Goss and Defense Secretary Donald Rumsfeld similar to the battles already faced, and lost, by DHS.*[214]

Whether state, local, and tribal law authorities will fare any better than the Department in its dealings with the IC is an open question, but as U.S. News and World Report correspondent Chitra Ragavan commented during a 9/11 Public Discourse Project panel discussion this summer, the situation does not look promising. "[W]hile information sharing has gotten to be considerably better, a lot of police officers, for instance, tell us that the biggest challenge they face is getting the FBI to share information with DHS and getting DHS to share it with them," she stated.[215] "[T]hey don't trust this relationship because of this incredible rivalry and turf wars between the two agencies. They're unclear as to how much information is being shared . . ."[216]

Given these divisions, it is perhaps not surprising that the fifteen agencies that comprise the IC have adopted a host of different ways to sanitize law enforcement intelligence – approaches that often conflict and typically fail to keep state, local, and tribal law enforcement officers in the loop.[217] "Because information protection standards vary, decisions on reconciling the need to protect information with the need to share information are applied inconsistently, contributing to information segregation rather than integration," Russack stated during his July testimony before the Senate Judiciary Committee.[218] Crowell concurred, noting that the various approaches to declassification within the IC are ad hoc and inefficient at best:

---

[214] Daniel B. Prieto, "Ending Interagency Feuds," Washington Times, May 26, 2005, available at http://www.washingtontimes.com/op-ed/20050525-090950-8080r.htm.

[215] Chitra Ragavan, Remarks at the 9/11 Public Discourse Project Panel Discussion on Proposed Changes to the CIA and FBI Following the Recommendations of the 9/11 Commission (June 6, 2005), available at http://www.9-11pdp.org/ua/2005-06-06_ragavan.pdf.

[216] Id.

[217] Crowell, supra note 175.

[218] U.S. Congress. Senate. Committee on the Judiciary. Hearing on FBI Oversight. 109th Cong., 1st sess., 2005 (statement of John A. Russack, Program Manager, Information Sharing Environment) (on file with author).

> *Another problem with the current system is that each agency has its own classification practices, which leads to cultural tensions when agencies attempt to share information with each other. Government agencies currently rely on processes for 'sanitizing' classified information so that it can be shared with other agencies. Some federal agencies sanitize some reports to remove source and method information. But the sanitized version is often still classified, and is usually designed for dissemination only to other federal agencies. Sanitization does not generally occur as a matter of course for many agencies, and no agency, to our knowledge, regularly produces a sanitized version of information that is unclassified and appropriate for wide-scale dissemination to state, local, and private sector entities. The sanitation process is also often slow and cumbersome.*[219]

The CIA, FBI and NSAs' separate write-to-release policies referenced above are just the tip of the iceberg in this regard. While the FBI's new write to release policy "is a step in the right direction," Crowell added, "an agency-by-agency approach will not work. What is needed is a national framework that would enable change across the government as a whole and with state and local authorities as well to overcome cultural barriers to information sharing."[220] Gilman Louie, a member of the Markle Foundation's National Security Task Force and president of In-Q-Tel Inc., a non-profit venture capital fund supported by the CIA, also believes that "[t] he greatest challenge will be getting cooperation from federal agencies, whose internal policies for protecting and releasing information may be in conflict with a government wide policy . . ." [221] Louie questions, however whether the DNI or Russack actually have the authority to compel federal agencies to comply with a federal information-sharing policy.[222] "Without that authority," he stated, "it becomes very difficult to solve this problem. If we need consensus, it may take too long."[223] John Jay Carafano, a senior fellow at the Heritage Foundation, is even less enthusiastic about the prospects for a concerted approach in this area, dismissing the planned policy as "a pie-in-the-sky idea" that is "not a reasonable requirement."[224]

These challenges foreshadow yet another hurdle to effective information sharing. Even if all the intelligence agencies adopted a common, consistent policy for disseminating law enforcement intelligence, and even if all the cultural divisions that still dog the IC disappeared, it is not at all clear that the IC even knows what kinds of information would be most valuable to their state, local, and tribal partners. Historically, most intelligence analysis conducted by the IC has been destined for high-level federal

---

[219] Crowell, supra note 175.
[220] Id.
[221] Alice Lipowicz, "Drift Into Nothingness," WashingtonTechnology.com (Oct. 10, 2005), at http://www.washingtontechnology.com/news/20_20/federal/27160-1.html.
[222] Id.
[223] Id.
[224] Id.

policymakers – not first responders in the field.[225] Without some input from these new intelligence consumers, however, the result might be useless data dumps on first responders made in the name of "information sharing." "The caveat is to make sure the information in the intelligence products is essential and reaching the right consumer," Carter observed.[226] "If law enforcement officers are deluged with intelligence reports, the information overload will have the same outcome as not sharing information at all," he added.[227] "If officers are deleting intelligence products without reading them, then the effect is the same as if it had never been disseminated."[228]

In short, all the tearline, write-to-release, and other information sharing guidelines in the world will fail to secure the homeland if they do not ensure that specific, actionable law enforcement intelligence is delivered to the right officers in the right place at the right time. It will be impossible to avoid overwhelming state, local, and tribal law enforcement officers under mountains of information, however, without a clear understanding of what those officers really need. As Peter A. Modafferi, Chief of Detectives of the Rockland County, New York, District Attorneys Office has observed:

> *Policymakers in Washington speak in terms of getting law enforcement Intelligence "down" to state, local, and tribal law enforcement officers. It's not that simple. We are not interested just in what they know. All of us – at every level of government – have to be interested in what we all know. We have to recognize that "all information is local." Information is a valuable resource and turning that information into actionable intelligence is not solely the task of the Intelligence Community. We, jointly, have to develop not only policies but also an implementation plan that will bring all law enforcement into the intelligence process. The biggest issue and obstacle to achieving this is not technology but history and culture.*[229]

Chief Polisar of the Garden Grove, California Police Department echoed these sentiments exactly when addressing his own frustrations with the Department:

> *The last thing we need at the Department of Homeland Security is more admirals, more generals, or more federal agents calling the shots. There are few if any state and local law enforcement experts in positions of authority at the Department; consequently, there is a failure to completely appreciate the abilities, concerns, and needs of cops on the beat. While we've heard a lot of lip service about reaching out to state and locals,*

---

[225] See Deborah G. Barger, Toward a Revolution in Intelligence Affairs 21, RAND Corporation, National Security Research Division (2005), available at http://www.rand.org/pubs/technical_reports/2005/RAND_TR242.pdf.

[226] Carter, supra note 10; Chapter 6: Law Enforcement Intelligence Classification, Products, and Dissemination at 86.

[227] Id.

[228] Id.

[229] Telephone Interview with Peter A. Modafferi, Chief of Detectives, Rockland County, New York District Attorneys Office (Nov. 16, 2005).

> *these well-meaning folks don't know where to start most of the time. Even if the Department were able to create an effective means of two-way communication between the federal government and state and locals – something that remains to be seen – I am not at all confident that the Department would know what to do with any information we might be able to get to them. There's a big disconnect here that needs attention.*[230]

Divining the needs of state, local, and tribal law enforcement officers without conferring with them accordingly would be a senseless waste of time. Establishing an information sharing mechanism that does not allow those officers to share information with the IC, moreover, would be pointless. As the Safe Cities Project recently noted, "Counterterrorism intelligence sharing will not be effective until police have a single venue for two-way information sharing between local, state, and federal agencies."[231] While what that "single venue" should look like, where it should be located, and how it should operate are open questions, the UK Intelligence Community's experience offers some answers.

A Vertical Intelligence Terrorism Analysis Link (VITAL) for Information Sharing

In order to overcome the structural and cultural obstacles to effective information sharing, it is necessary to change the IC's view of what information sharing is all about. As the authors of the Robb-Silberman Report commented:

> *The term information "sharing" suggests that the federal government entity that collects the information "owns" it and can decide whether or not to "share" it with others. This concept is deeply embedded in the Intelligence Community's culture. We reject it. Information collected by the Intelligence Community – or for that matter, any government agency – belongs to the federal government. Officials are fiduciaries who hold the information in trust for the nation. They do not have authority to withhold or distribute it except as such authority is delegated by the President or provided by law. As we have noted elsewhere, we think that the Director of National Intelligence could take an important, symbolic first step toward changing the Intelligence Community's culture by jettisoning the term "information sharing" itself – perhaps in favor of the term "information integration" or "information access."*[232]

One way to shift the focus from "information sharing" to "information access" is to provide state, local, and tribal law enforcement officers with a voice in the intelligence

---

[230] Telephone Interview with Joseph Polisar, Chief of Police, Garden Grove, California Police Department (Nov. 22, 2005).
[231] Safe Cities Project, Hard Won Lessons: Problem-Solving Principles for Local Police 6 (May 2005) [hereinafter Safe Cities Project Report], available at http://www.manhattan-institute.org/pdf/scr_02.pdf.
[232] Robb-Silberman Report, supra note 5 at 430.

analysis process. Specifically, they need a common channel through which they not only can receive intelligence from their federal partners but also can forward their own resources to those partners.[233]

Thomas S. Blanton, Executive Director of the National Security Archive at George Washington University, argued recently that a Declassification Center should be established at the National Archives in order to make more government information available to the public, stating, "If you create a power center for creating and holding secrets, like the new intelligence czar, then you need a counter center for declassifying secrets."[234] While Blanton was not discussing the information sharing challenges that exist between the IC and law enforcement, the same principle applies: the U.S. needs a formal team of experts at the federal level – drawn from the ranks of state, local, and tribal law enforcement officers nationwide – who can review classified intelligence information; determine which intelligence information would be of assistance to law enforcement in their efforts to thwart terrorist attacks; sanitize that information in order to remove sensitive sources and methods; and rapidly relay the end product the appropriate audience. The British experience on this front is highly instructive.

The British Approach

The 9/11 attacks in the United States spurred a series of urgent reviews of the UK's counterterrorism capabilities and structures.[235] One such review concentrated on the relationship between the nation's police services, which largely investigate criminal activity,[236] and the Security Service (MI5),[237] which works to protect the country against "covertly organised threats to national security, including terrorism, espionage, and the proliferation of weapons of mass destruction."[238] Cooperation between these two entities had traditionally been coordinated and facilitated by the police Special Branch,[239] which

---

[233] Cilluffo, supra note 209 at 71.

[234] U.S. Congress. House. Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations. Hearing on Emerging Threats: Overclassification and Pseudo-classification. 109th Cong., 1st sess., 2005 (statement of Thomas S. Blanton, Director, National Security Archive, George Washington University, available at http://reform.house.gov/UploadedFiles/Blanton%20Shays%20testimony%202%20March%202005.pdf).

[235] Keith Weston, Police International Counter Terrorism Unit (PICTU) Background Document 1 (Aug. 19, 2005) (unpublished manuscript, on file with author).

[236] UK Police Service Home Page, The Different Roles, available at http://www.policecouldyou.co.uk/default.asp?action=article&ID=45 (last visited Nov. 22, 2005) [hereinafter "UK Police Service Home Page]. Each county in the UK has its own police force while the Metropolitan Police operates within the Greater London area. Don Philpott, "The Global Terrorist Threat: United Kingdom's Homeland Security," Homeland Defense Journal, June 2004, at 55.

[237] UK Police Service Home Page, supra note 236.

[238] MI5 The Security Service Home Page, About MI5, available at http://www.mi5.gov.uk/output/Page7.html (last visited Nov. 21, 2005). "MI5 is responsible for all security matters within the UK and uses covert methods to obtain information about target organizations developing detailed knowledge over time about their key personalities, infrastructure, plans and capabilities," noted one observer. See Philpott, supra note 235 at 56. "MI6, otherwise known as the Secret Intelligence Service, is responsible for collecting secrets overseas." Id.

[239] Weston, supra note 235 at 1.

consists of specially trained and selected police officers on every UK police force who collect, assess, and disseminate intelligence on law enforcement issues.[240] The Special Branch's priority is to ensure that "front-line uniformed patrolling officers and detectives are briefed on threats, terrorist modus operandi and preventative operations aimed to deter, detect or disrupt terrorist activity."[241] Stated another way, "[T]he police Special Branches provide what is called the 'golden thread' linking the public duty to assist the police with the counter-terrorism process."[242] Despite this mechanism, many UK observers concluded that the Special Branch had at times failed to promote effective information sharing when it came to counterterrorism. Specifically, security marking classifications on reports; a lack of resources; a lack of coordination; and a "failure of imagination on the part of some key personnel within the police service" had on occasion prevented the Special Branch and the Security Service (MI5) from "engaging the wider police community in terrorism awareness and support activity."[243] The UK's Association of Chief Police Officers and Security Service (MI5) accordingly created the Police International Counter Terrorism Unit (PICTU) in December 2001 in order to address this perceived gap.[244]

PICTU is a main pillar of a 10-point counterterrorism program designed by Sir David Veness – Scotland Yard's former head of special operations and now the United Nations Under Secretary General for Safety and Security – to reflect what he described as the "seismic shift" in terrorist threats occasioned by 9/11.[245] PICTU was designed to coordinate the activities of the police Special Branch units throughout the UK in order to assist in the early assessment of perceived terrorist threats.[246] One of the main factors contributing to its creation was the recognition that the police service needed access to intelligence assessments in order to thwart terrorist attacks within the country.[247] Starting in February 2002, PICTU worked with various partners to analyze the reports that the UK Intelligence Community was producing in order to "identify those that had the potential to add value to police activity."[248] Toward that end, the Association of Chief Police

---

[240] Weston Sept. 1 Email, supra note 6. See Email from Keith Weston, former Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Dec. 3, 2005, 05:47:00 EDT) (on file with author).
[241] Weston Sept. 1 Email, supra note 6.
[242] Frank Gregory, Intelligence-Led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005, Real Instituto Elcano (2005), available at http://www.realinstitutoelcano.org/zonasanalisis.asp?zona=7&version=2&publicado=1. The Security Service (MI5) also sets the priorities for the gathering of counter-terrorist and other national security intelligence by the Special Branch, which serves as a key Security Service partner at the local level. Id.
[243] Weston, supra note 235 at 1-2.
[244] Id. at 1.
[245] Nick Hopkins, "Europe's Shared Security System," World Press Review, March 2002, available at http://www.worldpress.org/europe/0302guardian.htm.
[246] Nick Hopkins, "Yard Leads Plans for Europe Force to Track Al-Qaida," Guardian Unlimited, Jan. 10, 2002, available at http://www.guardian.co.uk/ukresponse/story/0.11017,630290,00.html.
[247] Weston, supra note 235 at 2.
[248] Id. The Association of Chief Police Officers (ACPO) represents the UK's most senior officers and set policies and standards for all the country's police forces. See Philpott, supra note 236 at 55. It also operates the Terrorism and Allied Matters Committee (TAM) that advises government on policies, training, and resources. Id.

Officers, Terrorism and Allied Matters Committee (ACPO-TAM) tasked PICTU with ensuring "[t]he effective dissemination of assessed intelligence relating to international terrorism of value to the National Co-ordinator for Terrorist Investigations, the National Coordinator for Special Branch and all UK police forces . . ."[249]

According to Keith Weston, the former Detective Chief Superintendent of PICTU, the unit quickly discovered that the UK Intelligence Community was often failing to keep law enforcement in the loop.[250] PICTU addressed this deficiency by injecting a police voice into the intelligence assessment process already underway at the UK's newly-established Counter Terrorism Analysis Centre (CTAC):

> *[PICTU's] analysis revealed that only 1 in 5 of the reports were being addressed to the police. Most of those were directed to the Metropolitan Police Special Branch (MPSB) on the erroneous assumption that they were then circulated to all police forces. The analysis also revealed that many more of the reports had information that could inform police strategies, particularly if sanitized and delivered with a lower protective marking. Given this unprecedented access to reports (often in draft stage), PICTU was able to offer advice on the relevance, protective marking and circulation of reports to police audiences. Within 9 months the proportion of reports addressed to police increased to 3 in 5. The majority of these reports were based on highly classified reports, but were issued in lower classification, allowing police officers to make operational use of the intelligence that had been collected. This transformation created additional work for the Security Service staff who produced the reports, as they needed to ensure that the disseminated intelligence did not compromise sensitive sources or sensitive methods of intelligence collection.*[251]

PICTU's findings led to regularly scheduled meetings designed to ensure that the intelligence needs of local police forces – i.e., to prevent terrorist attacks – are met.[252] During those still ongoing meetings, law enforcement officers and intelligence analysts (1) review intelligence reports produced by the Security Service (MI5); (2) identify evolving police intelligence requirements; and (3) monitor progress on the delivery of reports that support "Operation Fairway" – a program designed to review the effectiveness of the police response to international terrorist threats.[253]

PICTU is presently located within the Security Service (MI5) headquarters – an arrangement that has been beneficial to its information sharing focus.[254] As Weston notes, "The Service's logistical and administrative support to PICTU has been

---

[249] Weston, supra note 235 at 1.
[250] Id. at 2.
[251] Id. at 2-3.
[252] Id. at 3.
[253] Id.
[254] Id. at 11.

exemplary. The location of the Unit has greatly helped the access to key partners and enabled valuable personal working relationship to develop."[255] PICTU – which is "owned" by APCO-TAM and is staffed by both police officers from across the UK and Security Service (MI5) officers – works with the Security Service (MI5) and the Joint Terrorism Analysis Centre (JTAC) to ensure effective dissemination of assessed intelligence relating to international terrorism that is of value to the police service.[256]

PICTU today continues its work to reduce the terrorist threat and improve the police response to that threat by identifying, advancing, and reviewing national policing initiatives that are intended to make the UK "a hostile environment for terrorists."[257] In so doing, PICTU seeks to raise awareness of international counterterrorism issues at both strategic and tactical levels of the police service.[258] Toward that end, PICTU plays a key role in identifying "activity for all police forces from the emerging intelligence or research and, where there is no intelligence, monitoring the delivery of the national [counterterrorism] strategy through visits to police forces, gathering and following up feedback."[259] As part of its presentations to police, for example, PICTU sometimes uses open source material to inform the discussion when specific intelligence is lacking.[260] As Dr. Bruce Hoffman of the RAND Corporation observed:

> *[T]he job of this PICTU unit . . .is specifically to take all the classified reports and to find a way to disseminate them to the constabularies throughout the entirety of Britain. They way they do it is . . .look for open source reporting of incidents that they don't deem the classified remaining, they distribute these to the police forces. Or, in the worst case scenario, on their own they sort of boil down a white unclassified version of these reports and then distribute them widely, to give the local police at least some idea of why they're being placed on alert, and more specifically, what they should be looking for, because it's not enough just to place the police force on alert, they have to have specific information.*[261]

"By attending or organizing workshops, seminars and conferences to engage police officers and police staff at the senior management, middle management and practitioner level," Weston observes, "PICTU is able to increase awareness of the threat from international terrorism in the UK and to highlight the national counter terrorism strategy in an impactive way."[262] He adds that it is essential that this cyclical flow of information

---

[255] Id.
[256] Weston Sept. 1 Email, supra note 6; Keith Weston, New Threshold Terrorism – A UK Perspective 5 (January 2005) [hereinafter New Threshold Terrorism Manuscript] (unpublished manuscript, on file with author).
[257] New Threshold Terrorism Manuscript, supra note 256 at 5.
[258] Id.
[259] Weston, supra note 235 at 11.
[260] Weston Sept. 1 Email, supra note 6.
[261] Bruce Hoffman, Viewing Terror in Jerusalem From an International Perspective, Lecture Before the Jerusalem Institute for Israel Studies (June 30, 2003) at http://www.jiis.org.il/terror2.pdf at 15-16.
[262] Weston, supra note 235 at 3-4.

to and from the police forces and their intelligence partners be maintained in order to ensure the effectiveness of police responses to terrorist threats on a going forward basis.[263]

PICTU was a forerunner of JTAC,[264] which itself marked a major milestone in improving information sharing efforts between police forces and the UK Intelligence Community. Established in 2003, JTAC analyzes and assesses all intelligence relating to international terrorism – at home and overseas – and produces assessments of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies.[265] According to Professor Frank Gregory of the University of Southampton, JTAC represents, "[t]he most significant development in the analytical element of the UK's management of terrorism . . .," in large part because it has brought together various intelligence resources under one roof.[266] It is hoped that this collocation will create a shared identity that will help remove barriers to interagency intelligence sharing.[267] As Gregory notes:

> *JTAC operates under the authority of the Director General MI5 and it represents a specific move to break down institutional barriers between intelligence agencies by the processes of co-locating the analysts from all the intelligence agencies and other specialist agencies thus creating a new shared identity through JTAC membership. JTAC's remit is to provide long-term studies of international terrorism, for instance on the suicide bomber problem and immediate assessments of current threats. The Government conceives JTAC as the UK's centre of excellence and expertise on the threat from international terrorism and by the Autumn of 2003 JTAC was dealing with an average of 100 pieces of threat intelligence world-wide every week.*[268]

JTAC presently generates three main intelligence products: (1) country-based threat analyses and sector- or location-specific threat analyses for the UK which, from the available evidence, are used to set the security alert states for the UK; (2) analyses of

---

[263] Id. at 11.
[264] CTAC was folded into JTAC in June 2003 in an attempt to improve intelligence analysis coordination within the UK Intelligence Community. Report of St. Andrews/Southampton ESRC Project on the UK's Preparedness for Future Terrorist Attack: Some Major Research Issues and Findings (Economic & Social Research Council, Swindon, UK), July 2005, at 20, available at http://www.st-andrews.ac.uk/academic/intrel/research/cstpv/documents/Executive%20Summary.pdf. CTAC had been criticized after terrorist bombings in Bali of which it apparently had had some prior warning. Id.
[265] MI5 The Security Service Home Page, About MI5: Organisation, available at http://www.mi5.gov.uk/output/Page65.html (last visited Oct. 13, 2005).
[266] Gregory, supra note 242.
[267] Frank Gregory, Pre-emption and Protection: An Assessment of the Contribution of Intelligence Led Counter-Terrorism to UK Homeland Security Post 9/11 14 (December 2004) (unpublished paper presented to the 29th Annual Conference of the British International Studies Association at the University of Warwick) (on file with author).
[268] Gregory, supra note 242.

terrorist groupings and networks, including studies of key individuals; and (3) terrorism trends analyses.[269]

Unlike PICTU, which advises the UK Intelligence Community about what information would be of interest to police officers, JTAC actually undertakes the work of converting classified material to a format that is appropriate for police readership.[270] "Police officers within JTAC actively identify relevant JTAC reporting which could be used to raise awareness of terrorism among front line officers," Weston advises.[271] "The reporting is sanitized to disguise the source and remove any operational or sensitive items."[272] For example, while highly classified material might be relayed directly to the Special Branch within a particular police department for handling, it is not always possible to collect precise intelligence that provides opportunities for the police service to focus specific operations or initiatives.[273] In such instances, it is essential to have a system of communicating such non-precise intelligence for preventative purposes to those who have a need to know.[274] In the UK, this is achieved by the aforementioned "Operation Fairway" reports that JTAC disseminates to the police services in order to guide local operational and strategic responses:

> *The most useful type of reporting concerns terrorist methodology (e.g., hostile reconnaissance and other terrorist related activity) and generic target types. We believe that these areas are where officers engaged in core policing activities will be most likely to identify terrorist activity if their awareness levels are high enough. The intention is that activity which might be considered criminal or dismissed with a plausible excuse is at least considered from a terrorism perspective.*[275]

Raising general awareness about identifiable terrorist behavior is the core purpose of the reporting.[276] "[P]olice experience in the UK has shown that much of the terrorists' money comes from low-level crime," Weston explains.[277] "In such cases it is crucial that front-line law enforcement personnel are alerted to the key indicators that identify whether a crime that appears to be a low level fraud, could be a terrorist fund raising operation."[278] By contrast, reporting issued in response to a particular event – i.e., the July 7, 2005 bus and subway bombings in London – tends to be more "statement of fact" in nature and is typically issued to prevent law enforcement from having to rely solely on media reporting or dispel rumor.[279]

---

[269] Weston Aug. 19 Email, supra note 8.
[270] Weston, supra note 235 at 3.
[271] Weston Aug. 19 Email, supra note 8.
[272] Id.
[273] Keith Weston, International Terrorism – The British Police Strategy 2 (January 2005) (unpublished paper on file with author).
[274] Id.
[275] Weston Aug. 19 Email, supra note 8.
[276] Id.
[277] New Threshold Terrorism Manuscript, supra note 256 at 3.
[278] Id.
[279] Weston Aug. 19 Email, supra note 8.

To produce its thematic briefing reports, JTAC draws on the police officers assigned to its ranks who not only have real-world policing experience but also appropriate security access and terrorism expertise:

> *Police officers seconded to JTAC have the highest UK security clearance. They bring a police perspective to identifying JTAC reporting which is likely to be useful to front line officers and tailor the product to ensure the terminology, length, and detail are appropriate to the target audience. In this respect, it is very important that police officers who understand terrorism and the working environment of front line officers carry out this process.*[280]

JTAC works especially closely with PICTU in this regard.[281] "PICTU is continuing close liaison with JTAC to ensure the continued dissemination of 'user friendly' products for the wider police service," adds Weston.[282] "In support of that strategy arrangements were recently made by PICTU for secondments of police analysts to JTAC – a development greatly welcomed by JTAC management."[283] In other words, civilian police analysts who are already familiar with the process of identifying intelligence that would be of interest to police officers on the beat are now working within JTAC to assist in the intelligence review, sanitization, and dissemination process.[284]

Although JTAC does not produce unclassified reports for public distribution,[285] most of its reporting to front line officers is "be on the lookout"-type reporting that is passed at the "Restricted" level – the lowest of the four UK security classifications.[286] The "Restricted" classification covers material such as terrorist methodology, tactics, training, intentions, targeting, and personalities that – if disclosed – would prejudice an investigation or facilitate the commission of a crime.[287] As a general matter, it encompasses, "anything that comes from an authoritative [intelligence] source and gives the patrolling officer or the contingency planner more information than they would receive from reading a good quality newspaper or book."[288] Police officers do not submit to a special security clearance process in order to receive "Restricted" material; however, they would be subject to criminal penalties and/or police discipline if they leaked its content.[289] Given the relatively low level of classification of this material, JTAC

---

[280] Id.
[281] MI5 The Security Service Home Page, supra note 265.
[282] Weston, supra note 235 at 5.
[283] Id.
[284] Civilian police analysts are police staff who are not "sworn officers." They are either already trained analysts or are selected from existing staff and are trained to be analysts and are charged with interpreting a vast amount of data and assessing its usefulness, or otherwise, to an investigation. See Email from Keith Weston, former Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Dec. 5, 2005, 16:41:00 EDT) (on file with author).
[285] Weston Aug. 19 Email, supra note 8.
[286] Id.; Weston Sept. 1 Email, supra note 6.
[287] Weston Aug. 19 Email, supra note 8; Weston Sept. 1 Email, supra note 6.
[288] Weston Sept. 1 Email, supra note 6.
[289] Id.

forwards "Restricted" reports to non-law enforcement entities and personnel such as Customs, the Department of Health, and the Fire Service.[290]

JTAC reports generated at the "Restricted" level are shared with front line officers through the police Special Branches via a secure communications system.[291] The reports are further disseminated on police intranet systems that are capable of carrying such material.[292] Individual police departments typically blend the JTAC information into their own briefing material or use the JTAC reports on their own.[293] By contrast, intelligence information of a very precise and sensitive nature is not routinely disseminated to UK police forces. Instead, it is acted upon by the Security Service (MI5) itself.[294] "[A]t the stage when the intelligence becomes evidential in nature, i.e., there is now some substantive activity on which to base a prosecution," Weston explains, "the Security Service consults with the National Coordinator for Terrorist Investigations (a senior police officer) who then calls an Executive Liaison Group (ELG) to discuss how best to take the investigation forward."[295] The main priority in such an active intelligence operation is preserving public safety, but the same concern with protecting sensitive sources and methods applies.[296] "Executive action, i.e., further surveillance, leading to arrests, would then fall under the responsibility of the National Co-ordinator, supported by whichever police force where the activity is taking place," Weston advises. While JTAC would not be involved in disseminating information in this circumstance, the Security Service (MI5) itself would pass out information selectively to those police officers who have a "need to know" – albeit without disclosing sources and methods in most cases.[297] Following a terrorism-related arrest, however, JTAC would issue an Operation Fairway report for general distribution to police forces in order to explain the background to the arrest and the implications for protecting national security – i.e., that a suspect is in custody and the threat has been resolved; or that some suspects remain at large; that there are still weapons and explosives in circulation; and that police forces are to stay on alert given an increased threat.[298]

Applications in the United States

The United States already has a JTAC equivalent in the NCTC – initially a recommendation of the 9/11 Commission adopted by federal officials and now one of several new entities formally established by the 9/11 Act.[299] In order to promote

---

[290] Weston Aug. 19 Email, supra note 8; Weston Sept. 1 Email, supra note 6.
[291] Weston Aug. 19 Email, supra note 8.
[292] Id.
[293] Id.
[294] Email from Keith Weston, former Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Thomas M. Finan, Counsel and Coordinator, House Committee on Homeland Security (Nov. 22, 2005) (on file with author).
[295] Id.
[296] Id.
[297] Id.
[298] Id.
[299] Exec. Order No. 13,354, 69 Fed. Reg. 53,589 (Aug. 27, 2004); 9/11 Act, § 1021.

effective intelligence analysis, integration and information sharing, the 9/11 Commission had specifically recommended the creation of the NCTC in order to break "the mold of national government organization" by being "a center for joint operational planning *and* joint intelligence, staffed by personnel from the various [intelligence] agencies."[300] The 9/11 Commission likewise recommended that the NCTC should lead strategic analysis of all intelligence, foreign and domestic, pertaining to transnational terrorist organizations; should develop net assessments by comparing enemy capabilities and intentions against U.S. defenses and countermeasures; and should provide appropriate warnings to the public.[301] By housing representatives from the various agencies that comprise the IC under one roof, the NCTC leverages the intelligence capabilities of the CIA, the FBI, the Department, and other agencies in order to integrate and analyze intelligence information for the purpose of developing strategic plans to protect the homeland.[302] As one observer noted shortly after the creation of the NCTC's predecessor, the Terrorist Threat Integration Center (TTIC):

> *The TTIC will stand as the preeminent "fusion cell" for domestic intelligence in the U.S.; its charter will provide for all-source, integrated analysis to the FBI, "but also to the officials in state and local law enforcement who are essential partner in the fight against terrorism." Potentially, the center may stand as the quintessential conduit between the CIA, the FBI, DOD, the DHS, the rest of the interagency, and law enforcement officials throughout the United States.*[303]

By taking on these responsibilities, the NCTC today encompasses the Department's original intelligence analysis role as outlined in the Homeland Security Act of 2002, which was to "'access, receive and analyze law enforcement information, intelligence information, and other information . . . and to integrate such information' to identify terrorist threats to the United States."[304] Secretary Chertoff is on board with this approach. "I most definitely anticipate and want to have DHS play a role in NCTC," he recently stated, indicating that making that happen is "really just a question of finding the space and handling the logistics."[305]

Like the JTAC in the UK, the shared access to intelligence information at NCTC has been described as a "positive"[306] development "at the forefront" of the IC's

---

[300] **National Commission on Terrorist Acts Upon the United States**, **The 9-11 Commission Report** 403 (2004) [hereinafter **The 9-11 Commission Report**] (emphasis in origina1).
[301] Id. at 404.
[302] See Exec. Order No. 13,354, supra note 299.
[303] Tussing, supra note 199 at 12-13.
[304] Justin Rood, "Analysis: New Counterterror Center Proposals Make DHS Intel Efforts 'Irrelevant'," Page 15 (Sept. 30, 2004), *at* http://page15.com/2004/09/analysis-new-counterterror-center.html.
[305] Department of Homeland Security Organization Transcript, supra note 211.
[306] U.S. Congress. House. Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment. Hearing on Federal Support for Homeland Security Information Sharing: The Role of the Information Sharing Program Manager. 109th Cong., 1st sess., 2005 (prepared statement of Lee H. Hamilton, Former Vice Chair National Commission on Terrorist Attacks Upon the United States, available at http://homeland.house.gov/files/testimonyHamilton.pdf) [hereinafter Hamilton Information Sharing Program Manager Statement].

continuing information sharing efforts.[307] As the authors of the Robb-Silberman Report have noted, information sharing "has improved substantially since September 11," a development that "is in no small part due to the creation of the . . . NCTC and the increased practice of housing collectors and analysts together, which provides a real-world solution to some of the bureaucratic and institutional barriers that exist between the big intelligence-collecting agencies."[308] In other words, the NCTC – by requiring side by side cooperation of its staff members – is helping to forge a "unity of effort across the Executive Branch" aimed at defeating terrorism.[309] "The National Counterterrorism Center (NCTC)," Crowell observed, "is enhancing collaboration across the foreign intelligence/domestic information divide that was so detrimental to our efforts before 9/11."[310]

Unlike the JTAC in the UK, however, the NCTC serves only federal customers and is not in the business of sanitizing intelligence documents for dissemination to state, local, or tribal law enforcement.[311] "'We support the agencies that have vertical responsibility' for sharing information with state and local law enforcement," explained Russ Travers, the NCTC's Deputy Director.[312] "'We have been focused for the past two years on sharing between and amongst our federal partners. '"[313] The NCTC likewise does not include state, local, or tribal law enforcement officers among its ranks who might be able to identify intelligence information of use to threat prevention efforts and to disseminate that information in a user-friendly format.[314] Senator Pat Roberts has lamented these limitations, stating, "The NCTC is described as the Las Vegas of the intelligence community: What goes on at the NCTC stays at the NCTC . . ."[315] While recognizing the NCTC's value, Hamilton has also criticized its exclusively federal focus:

> *Agencies still control the information they produce. They view it as their property, rather than the property of the entire government, and the*

---

[307] Reuters, "U.S. Counterterror Agency Criticized on Info-Sharing (July 1, 2005), available at http://www.boston.com/news/nation/washington/articles/2005/07/21/us_counterterror_agency_criticized_on_info_sharing/.

[308] Robb-Silberman Report, supra note 5 at 14.

[309] Press Release, Senators Susan Collins and Joseph Lieberman, Senators Collins & Lieberman Express Concerns That Pentagon's Expanded Human Intelligence Capabilities "Could Undermine Congress's Vision For Intelligence Reform," (Jan. 26, 2005), available at http://www.fas.org/irp/congress/2005_cr/s012605.html.

[310] U.S. Congress. House. Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment. Hearing on Federal Support for Homeland Security Information Sharing: The Role of the Information Sharing Program Manager. 109th Cong., 1st sess., 2005 (prepared statement of William P. Crowell, Markle Task Force on National Security in the Information Age, available at http://www.fas.org/irp/congress/2005_hr/110805crowell.pdf) [hereinafter Crowell Statement].

[311] Patience Wait, "Where the Data Meets the Road," Government Computer News (Aug. 29, 2005), available at http://www.gcn.com/24_25/top-stories/36781-1.html.

[312] Id.

[313] Id.

[314] See Jim VandeHei, "Bush Taps Admiral as Chief of Counterterrorism Center," Washington Post, June 11, 2005, at A04 ("[The NCTC's] analysts come from the CIA, the FBI and the Department of Homeland Security, as well as other agencies. The CIA, the FBI, and other law-enforcement units are expected to carry out anti-terrorism operations based on information collected by the NCTC.").

[315] Reuters, supra note 307.

> *property of the American people. For information sharing to work, the right information must get to the right person at the right time. Moreover, information sharing with state and local authorities has only marginally improved.*[316]

In order to get law enforcement intelligence to the front line police and sheriffs' officers who need it most, the DNI should establish a PICTU-like unit that can analyze intelligence, identify what intelligence would be of interest to law enforcement from a preventative perspective, and sanitize that intelligence by removing sources and methods information so it can be disseminated to officers in the field. Like PICTU, such a Vertical Intelligence Terrorism Analysis Link (VITAL)[317] should be staffed by state, local, and tribal law enforcement officers who have real-world experience in criminal investigations and other matters who can (1) inform the intelligence analysis process by identifying intelligence information that would be of interest to officers conducting operational and strategic planning; (2) assist in the dissemination of both sanitized intelligence products and open source-based informational products to the appropriate police audience; and (3) educate not only the IC about law enforcement's particular needs but also front line officers about the IC's homeland security plans and priorities.[318] Because the U.S. does not have a Special Branch equivalent, VITAL should be located within the NCTC itself in order to ensure an effective information sharing nexus between the IC and the law enforcement community – precisely the arrangement that JTAC recently welcomed in the UK through the introduction of PICTU staff to its ranks.[319] Collocating VITAL at the NCTC would have similar key benefits.

First, collocation would ensure that the right information gets to the right people. As noted previously, intelligence analysts have historically created products for high-level federal policymakers – not police and sheriff's officers.[320] Because the NCTC is the fusion point for information held by the entire IC, VITAL staff can peruse the shared material, identify what is of relevance to law enforcement, and then work with NCTC staff to generate a version of the information at a "law enforcement sensitive" or other

---

[316] Hamilton Information Sharing Program Manager Statement, supra note 306 at 3.

[317] Information sharing among the various agencies that comprise the IC is often referred to as "horizontal information sharing." See William P. Dizard, III, "Information Sharing Networks Overlap as Policy Gels, GCN.com (June 29, 2004), available at http://www.gcn.com/vol1_no1/daily-updates/26420-1.html. Information sharing by those federal agencies with their state, local, and tribal law enforcement partners is often referred to as "vertical information sharing." Id. The vertical focus of the information sharing that VITAL would facilitate gives VITAL its name.

[318] To supplement the law enforcement presence, VITAL staff could also include representatives from state, local, and tribal government familiar with preventative intelligence needs in their communities, as well as similarly situated officials from the private sector.

[319] Weston, supra note 235 at 5. As presently written, the 9/11 Act prevents the DNI from disseminating intelligence information directly to state and local government officials. 9/11 Act, §§ 1011, Sec 102A(f)(1)(B)(iii); 1021, Sec 119(f)(E). In order to remove any impediment to VITAL's creation or operation, Congress should amend the 9/11 Act to clarify that VITAL may disseminate – subject to appropriate civil liberties and privacy safeguards – sanitized intelligence information (i.e., without sources and methods information) to state, local, and tribal law enforcement officers that is relevant to identifying potential terrorists and thwarting potential terrorist attacks.

[320] See Barger, supra note 225 at 21.

unclassified designation.[321] Indeed, the goal of sanitizing sources and methods from classified documents is to provide specific and actionable intelligence information to law enforcement officers so they can make operational use of it. Instead of unloading unhelpful data dumps on law enforcement, VITAL will help target particular documents for sanitation and dissemination – avoiding the problem of overwhelming police and sheriffs' officers with too many pieces of paper that might go unread.[322] By drawing upon the intelligence "pool" at NCTC, moreover, VITAL will bypass the myriad problems caused by the various intelligence agencies adoption of multiple approaches to tearlines, write-to-release policies, and information sharing guidelines.[323] Like PICTU, VITAL accordingly would offer an effective and trusted mechanism to corral an orderly flow of information to and from the law enforcement community.

Second, collocation would establish VITAL as a critical link between the law enforcement and intelligence communities for information sharing purposes. Because VITAL – like PICTU – would be staffed by law enforcement officers from all over the country, it could leverage those officers' well-established relationships with colleagues and friends in the field.[324] Those relationships would likely continue to grow as a result of regular VITAL meetings with those officers, where their concerns could be aired and where the IC's own homeland security perspectives could be shared.[325] Moreover, because many VITAL staffers would already be familiar with front line law enforcement officers, they likely would be a helpful point of contact for those officers who wish to relay information to the IC. Information funneled from law enforcement to VITAL could then be passed on to other NCTC personnel for (1) referral to the FBI and the appropriate JTTF and ATAC for investigative action; or (2) inclusion within the overall intelligence mosaic as a preventative intelligence resource.[326]

Third, collocation would help develop a community of trust. By working together with NCTC staff from throughout the IC, VITAL staff would be uniquely positioned to educate analysts and others from the various intelligence agencies that comprise the NCTC about what kind of information law enforcement really needs.[327] As in PICTU,

---

[321] See Global Justice Information Sharing Initiative, International Association of Law Enforcement Intelligence Analysts, Inc., Law Enforcement Analytic Standards 20 (Nov. 2004), available at http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf ("Sensitivity levels relate to the need to keep secret the information held. In law enforcement, gradients now used include 'Law Enforcement Sensitive,' 'Sensitive But Unclassified,' 'For Official Use Only,' 'Confidential,' and 'Open Source.'"). Unlike the UK, the US does not appear to have adopted any generally applicable criminal or disciplinary sanction for the release of law enforcement sensitive information to the public. To the extent that law enforcement sensitive information to be disseminated through VITAL cannot be effectively generated without some protection from public disclosure – even after sources and methods have been excised from the material – Congress should consider appropriate penalties for disclosure under those circumstances.

[322] Carter, supra note 10; Chapter 6: Law Enforcement Intelligence Classification, Products, and Dissemination at 86.

[323] Crowell Statement, supra note 175.

[324] Weston Sept. 1 Email, supra note 6; Weston, New Threshold Terrorism Manuscript, supra note 255 at 5.

[325] Weston, supra note 235 at 3.

[326] Another logical conduit for information flows from VITAL is the Department's Homeland Security Information Network (HSIN), which links approximately 150 law enforcement agencies that have major intelligence analysis departments. See Wait, supra note 311.

[327] Modafferi Interview, supra note 229; Polisar Interview, supra note 230.

the day-to-day interactions between staffs would provide the IC with a deeper appreciation of those requirements and would likely encourage analysts to generate documents at the outset with an eye toward a law enforcement audience. In that way, VITAL could act as a catalyst to move the IC from a "need to know" mentality to the much discussed but still unrealized "need to share" environment.[328] VITAL thus would help overcome the ownership and control issues that have continued to plague the IC and consequently would mark a major shift from the "federal-centric" focus of most domestic intelligence operations today.[329]

More generally, VITAL would bypass many of the aforementioned information sharing challenges. For example, VITAL would effectively eliminate the problems occasioned by providing security clearances to all law enforcement officers everywhere. By introducing a discrete contingent of law enforcement officers at the NCTC, numbering perhaps 50 people, VITAL would limit the number of security clearances that would need to be vetted to a very small group. Because VITAL would ensure the dissemination of sanitized law enforcement intelligence to targeted law enforcement audiences, the vast majority of officers in the field would no longer need clearances themselves – a development that would help communities avoid the confusion, consternation, and costs that the vetting processes have generated to date. In addition, VITAL would obviate the need for NDAs altogether. Because VITAL would ensure the generation and dissemination of sanitized intelligence documents that do not include sensitive source or method information, there essentially would be no "classified" information for a NDA to protect. Finally, VITAL not only would fill in the information sharing "blanks" in communities not adequately serviced by a local JTTF but also would supplement the information already available to JTTFs, ATACs, and TEWs by helping to generate audience-appropriate reports for those entities.

Most importantly, VITAL would overcome federal policymakers' apparent inability to get the IC on the same information sharing page. Instead of generating another guideline to create guidelines – an approach that casts doubt on the government's ability to obtain full cooperation from the IC for this purpose – VITAL would shift the focus. Specifically, VITAL would establish law enforcement itself as a main driver of the intelligence products being shared with state, local, and tribal authorities by looping front line officers directly into the intelligence identification, analysis, and dissemination process. Like PICTU, VITAL therefore would represent a concrete step to promote information sharing that could have immediate dividends for the nation's homeland security efforts.

[328] Baird, supra note 187.
[329] Tussing, supra note 199 at 12-13.

Conclusion

It has been over four years since the 9/11 attacks. Despite many invitations to do so since then and despite much lip service in return, the federal government has squandered several opportunities to develop uniform standards for converting classified law enforcement intelligence information into an unclassified or "less classified" format for use by state, local, and tribal authorities. Police and sheriffs' officers need speedy access to that intelligence – particularly preventative intelligence – in order to maximize their ability to detect terrorists in their midst and to thwart their plans. Given the apparent inability of federal officials to complete this critical task – by honoring their obligations under the Homeland Security Act, the 9/11 Act, and otherwise – the U.S. should adopt a fresh approach by following the example of the UK's PICTU organization, a proven model of how to make effective information sharing a reality. A VITAL unit collocated at the NCTC would capture the best aspects of both PICTU and JTAC and would help move the country closer to the two-way flow of information between the IC and the law enforcement community that is a necessary prerequisite to securing the homeland.