Order Code RL34070

CRS Report for Congress

Fusion Centers: Issues and Options for Congress

Updated January 18, 2008

John Rollins
Specialist in Terrorism and International Crime
Foreign Affairs, Defense, and Trade Division

Prepared for Members and
Committees of Congress

Fusion Centers: Issues and Options for Congress

Summary

Although elements of the information and intelligence fusion function were conducted prior to 9/11, often at state police criminal intelligence bureaus, the events of 9/11 provided the primary catalyst for the formal establishment of more than 40 state, local, and regional fusion centers across the country.

The value proposition for fusion centers is that by integrating various streams of information and intelligence, including that flowing from the federal government, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people, economic infrastructure, and communities can be developed and translated into protective action. The ultimate goal of fusion is to prevent manmade (terrorist) attacks and to respond to natural disasters and manmade threats quickly and efficiently should they occur. As recipients of federal government-provided national intelligence, another goal of fusion centers is to model how events inimical to U.S. interests overseas may be manifested in their communities, and align protective resources accordingly. There are several risks to the fusion center concept — including potential privacy and civil liberties violations, and the possible inability of fusion centers to demonstrate utility in the absence of future terrorist attacks, particularly during periods of relative state fiscal austerity.

Fusion centers are state-created entities largely financed and staffed by the states, and there is no one "model" for how a center should be structured. State and local law enforcement and criminal intelligence seem to be at the core of many of the centers. Although many of the centers initially had purely counterterrorism goals, for numerous reasons, they have increasingly gravitated toward an all-crimes and even broader all-hazards approach. While many of the centers have prevention of attacks as a high priority, little "true fusion," or analysis of disparate data sources, identification of intelligence gaps, and pro-active collection of intelligence against those gaps which could contribute to prevention is occurring. Some centers are collocated with local offices of federal entities, yet in the absence of a functioning intelligence cycle process, collocation alone does not constitute fusion.

The federal role in supporting fusion centers consists largely of providing financial assistance, the majority of which has flowed through the Homeland Security Grant Program; sponsoring security clearances; providing human resources; producing some fusion center guidance and training; and providing congressional authorization and appropriation of national foreign intelligence program resources, as well as oversight hearings. This report includes over 30 options for congressional consideration to clarify and potentially enhance the federal government's relationship with fusion centers. One of the central options is the potential drafting of a formal national fusion center strategy that would outline, among other elements, the federal government's clear expectations of fusion centers, its position on sustainment funding, metrics for assessing fusion center performance, and definition of what constitutes a "mature" fusion center. This report will be updated.

Contents

List of Figures

List of Tables

A Methodological Note

Research for this report included a review of literature related to state and regional fusion centers, primary source interviews with the majority of state fusion center leaders and operational directors, as well as with stakeholders within the federal government, including Intelligence Community (IC) organizations, Department of Homeland Security (DHS) and the Government Accountability Office (GAO) officials. In the interest of engaging in open dialogue with the centers, the conversations were conducted on a "not for attribution basis." The inherent limitations of the survey method are acknowledged, but were adopted in the interest of efficiency and effectiveness. Other stakeholders and interested observers of state fusion centers outside the government, including individuals in academia, the American Civil Liberties Union (ACLU), and state and local law enforcement were also consulted. Primary source interviews were conducted by the authors and were based on a survey they developed.

Fusion Centers: Issues and Options for Congress

Introduction

The creation of post-9/11 intelligence/information[1] fusion centers[2] does not represent a totally new concept, but suggests an extension of pre-9/11 state and local law enforcement intelligence activities. Most state police/bureau of investigation agencies have run intelligence or analytic units for decades. Many of the fusion centers examined for this report were the outgrowth of those units, prompting some to refer to fusion centers as 'state police intelligence units on steroids." Conceptually, fusion centers differ from their predecessors in that they are intended to broaden sources of data for analysis and integration beyond criminal intelligence, to include federal intelligence as well as public and private sector data. Furthermore, fusion centers broaden the scope of state and local analysis to include homeland security and counterterrorism issues.

---

[1] Intelligence is information to which value has been added through analysis and is collected in response to the needs of policymakers. At the most generic level, there are two types of intelligence: raw and finished. Raw intelligence is that which has not been vetted, verified and validated. Finished intelligence, which includes information of unknown credibility, has been through an analytical process which has resulted in conclusions and judgments being made. As opposed to evidence, which is generally gathered in support of a prosecution, intelligence is gathered to inform policymakers and those individuals responsible for taking actions, including national security, law enforcement and public safety officials. While intelligence may occasionally be introduced into legal proceedings, generally it is not. The distinction between intelligence and information is discussed at length in **Appendix A**.

[2] The Fusion Center Guidelines define a fusion center as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, August 2006, available from [http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf], accessed on June 26, 2007, p. 2. Some apply this definition broadly to include any multi-jurisdictional anti-crime or response effort that may utilize intelligence and/or information, to include federally-owned and operated collaborative efforts, like FBI-led Joint Terrorism Task Forces (JTTFs) or High Intensity Drug Trafficking Area (HIDTA). The authors, however, limit their discussion of fusion centers to those 40+ largely state and regional entities created to enhance the ability of the jurisdiction to prevent, mitigate, and in some cases, respond and recover, from man-made threats, attacks, and natural disasters.

Despite being an expansion of existing sub-federal intelligence/information activities, fusion centers represent a fundamental change in the philosophy toward homeland defense and law enforcement. The rise of fusion centers is representative of a recognition that non-traditional actors — state and local law enforcement and public safety agencies — have an important role to play in homeland defense and security. In addition, there has been a shift towards a more proactive approach to law enforcement in the United States.

Numerous national strategies have assessed the primary threat to U.S. national security as terrorism, both at home and abroad.[3] Indeed, the National Strategy on Homeland Security provides that "the American People and way of life are the primary targets of our [terrorist] enemy and our highest protection priority."[4] The means for combating this threat are broad and encompass all elements of national power, to include non traditional sectors. From a law enforcement perspective, it has been argued that state and regional intelligence fusion centers, particularly when networked together nationally, represent a proactive tool to be used to fight a global jihadist adversary which has both centralized and decentralized elements. This network of fusion centers is envisioned as a central node in sharing terrorism, homeland security, and law enforcement information with state, local, regional, and tribal law enforcement and security officials.[5]

Today, there are over 40 intelligence fusion centers across the country (see **Appendix B** for a map and list of these centers). Research suggests that there is no "one-size-fits-all" model for these centers and there are significant differences between them. There are, however, some common themes, and more importantly, common questions, that arise when examining fusion centers, to include:

- Do fusion centers solve the pre-9/11 information sharing problems, and as such, make Americans safer?

---

[3] For example, the National Strategy on Counterterrorism states that "The paradigm for combating terrorism now involves the application of all elements of our national power and influence. Not only do we employ military power, we use diplomatic, financial, intelligence, and law enforcement activities to protect the Homeland and extend our defenses, disrupt terrorist operations, and deprive our enemies of what they need to operate and survive." See *The National Strategy for Combating Terrorism*, September 2006, p. 1. and According to the Director of National Intelligence (DNI), "Terrorist threats to the Homeland, to our national security interests, and to our allies remain the pre-eminent challenge to the Intelligence Community...." See "Annual Threat Assessment of the Director of National Intelligence," Testimony of Ambassador John D. Negroponte, Before the Senate Select Committee on Intelligence, January 11, 2007, p. 2.

[4] See *The National Strategy on Homeland Security*, July 2002, p. 7.

[5] This vision is promoted by the Program Manager - Information Sharing Environment (PM - ISE), which was created by Intelligence Reform and Terrorism Prevention Act of 2004, Section 1016 and was placed under the administration of the Office of the Director of National Intelligence. The functions, but not necessarily the authorities, of the ISE transcend the boundaries of the federal intelligence and law enforcement communities. See Chapter Seven "Sharing with Partners Outside the Federal Government," in *Information Sharing Environment Implementation Plan*, Office of the Director of National Intelligence, November 2006.

- Can fusion centers work if they aren't part of an integrated philosophy of intelligence and security?

- Who "owns" and benefits from fusion centers? Who should staff, fund, and oversee them? What role, if any, should fusion centers play in the Intelligence Community (IC), and what role should federal agencies play in fusion centers, to include funding?

- Do fusion centers represent a shift in the security v. civil liberties pendulum? How active and pro-active, if at all, should fusion centers be in the collection of intelligence that is not directly tied to a specific and identifiable criminal act?

- There is no single model for how each center is structured or operates. Is some basic level of common standards necessary in order for fusion centers to offer a national benefit? Moreover, does the federal government have an integrated national strategy towards fusion centers?

- Is the current configuration of 40 plus fusion centers, with, in some cases, several operating within one state, the most efficient organizational structure?

- Is the current approach to creating, authorizing, funding, and supporting fusion centers sustainable? What are the risks to the fusion center concept and how have those risks been specifically weighed and balanced against the stated goals of fusion center operations?

In order to provide context for the analysis of these fundamental questions, this report will highlight how the concept and development of these centers continue to evolve, as well as provide an overview of current national trends in fusion centers, the federal role in supporting such centers, and the role of the private sector. Finally, the report will provide Congress with a number of legislative options for consideration. Prior to examining these topics, it is necessary to consider the value proposition these centers pose, as well as potential risks to fusion center development.

Fusion Center Value Proposition

Conceptually, the argument that fusion centers represent a vital part of our nation's homeland security relies on at least four presumptions:

- Intelligence, and the intelligence process, plays a vital role in preventing terrorist attacks.

- It is essential to fuse a broader range of data, including non-traditional source data, to create a more comprehensive threat picture.

- State, local, and tribal law enforcement and public sector agencies are in a unique position to make observations and collect information that may be central to the type of threat assessment referenced above.

- Having fusion activities take place at the sub-federal level can benefit state and local communities, and possibly have national benefits as well.

DHS's Value Proposition. The Department of Homeland Security (DHS) has stated that the value of fusion centers to both DHS and state and local authorities includes a number of common and distinct functions. The following four areas were assessed by DHS as being common benefits fusion centers would yield to DHS and state and local authorities:

- Clearly defined information gathering requirements.
- Improved intelligence analysis and production capabilities.
- Improved information/intelligence sharing and dissemination.
- Improved prevention, protection, response, and recovery capabilities.[6]

DHS also outlined areas of how it and state and local authorities would benefit uniquely from participation in the fusion centers. Unique benefits to DHS include:

- Improved information flow from state and local entities to DHS.
- Improved situational awareness.
- Improved access to local officials.
- Consultation on state and local issues.
- Access to non-traditional information sources.

According to DHS, the unique benefit of fusion centers to state and local authorities includes:

- Improved information flow from DHS to states and localities.
- Increased on-site intelligence and DHS law enforcement expertise and capabilities.
- Clearly defined DHS entry point.
- Insight into federal priorities.
- Participation in dialogue concerning threats.

The extent to which DHS's vision of the fusion center value proposition has developed will be addressed throughout this report. Given that the tenure of DHS Office of Intelligence and Analysis (OIA) personnel detailed to fusion centers is less than one year, it could be argued that it may be premature to assess the extent to which DHS's vision for fusion center payoffs is being realized. However, as will be further explained below, research indicates that DHS personnel are being used

---

[6] DHS, *Support Implementation Plan for State and Local Fusion Centers: Executive Summary*, June 2006.

currently more as a "clearly defined DHS entry point," than as tools to improve "...intelligence analysis and production capabilities." Moreover, the development of a process for gathering information according to clearly defined information requirements in fusion centers remains nascent.

Importance of Intelligence and Intelligence Sharing. To briefly expand upon the four presumptions which are often cited in arguments that fusion centers are valuable to homeland security, it is important to first focus on the role of intelligence in homeland security, especially with regard to prevention efforts. At the First Annual National Fusion Center Conference, Secretary Chertoff reiterated to the hundreds of state and local conference participants that he views intelligence as an early warning system that allows public safety officials to get a jump on the adversary.[7] The 9/11 Commission states, "Not only does good intelligence win wars, but the best intelligence enables us to prevent them from happening altogether."[8] All major post-9/11 government reorganizations, legislation, and programs have emphasized the importance of intelligence in preventing, mitigating, and responding to future terrorist attacks. This includes the creation of the Department of Homeland Security, specifically the Department's Office of Intelligence and Analysis, the passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2005 (P.L. 108-458), intelligence sharing provisions of the USA PATRIOT Act (P.L. 107-56), as well as the creation of the Intelligence Sharing Environment (ISE), among numerous other developments.

Importance of Fusion, Including Non-Traditional Intelligence/Information. Another presumption that is often cited is that to prevent attacks intelligence needs to include a broad range of data, including that from non-traditional sources — state and local homeland security-related personnel and the private sector. The Commission found that the September 11th attack plot:

> fell into the void between foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States.[9]

As such, the 9/11 Commission concluded there was a necessity for fusing domestic and foreign intelligence.

Fusing foreign intelligence with a wide spectrum of domestic information is the stated primary purpose of most fusion centers. Locally gathered information collected from a broad array of law enforcement, public health and safety, as well as private sector sources, is fused with intelligence collected and produced by the

---

[7] Derived from CRS transcription of Secretary Chertoff's Keynote Address to the first annual National Fusion Center Conference, March 6, 2007.

[8] *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, Authorized Edition (New York: WW Norton & Company, 2004), 420.

[9] *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, p. 263.

federal Intelligence Community to better understand threat and assist in directing security resources. The authors of the *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* stated:

> Data fusion involves the exchange of information from different sources — including law enforcement, public safety, and the private sector — and, with analysis, can result in meaningful and actionable intelligence and information. The fusion process turns this information and intelligence into actionable knowledge.[10]

The Homeland Security Advisory Council (HSAC) finds that this process should be continual, "...More than one-time collection of law enforcement and/or terrorism-related intelligence information and it goes beyond establishing an intelligence center or creating a computer network....[11] Furthermore, HSAC believes that out of the fusion process,

> one of the principal outcomes should be the identification of terrorism-related leads — that is, any nexus between crime-related information and other information collected by State, local, tribal, and private entities and a terrorist organization and/or attack.[12]

By fusing state and local information with federal threat intelligence, it could be argued, fusion centers serve as a vital linkage or "translator" for state and local authorities. For example, when a bombing occurs overseas, it can be very helpful for *modus operandi* and other tactical information surrounding that bombing to be communicated to states and localities in a timely fashion so they may align their protective resources accordingly. The fusion centers, through their connectivity with the federal Intelligence Community via either systems and/or federal personnel collocated at the centers, can serve as the single focal point for timely dissemination of that information. The imperative, according to Charles Allen, Chief Intelligence Officer at DHS, is to push the defensive perimeter outward. According to Allen:

> Our ability to move, analyze, and act on information is our greatest strength. And, we must use the (national fusion center) information in that network to push our defensive perimeter outward.[13]

While providing an important indication and warning function in a counterterrorism sense, the fusion process can also be harnessed for preventing other types of crime, and/or responding to natural disasters as will be discussed in-depth below.

---

[10] See *Fusion Center Guideline: Developing and Sharing Information and Intelligence in a New Era,* August 2006, p.

[11] See U.S. Department of Homeland Security, Homeland Security Advisory Council, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*, April 28, 2005, p. 3.

[12] Ibid.

[13] Derived from CRS transcription of speech by Charles Allen at the First Annual National Fusion Center Conference, March 6, 2007.

Unique Role of State, Local and Tribal (SLT) Public Sector. It has been argued that state, local, tribal law enforcement, first responders, and other public and private sector entities are uniquely positioned to collect information to identify emerging threats and assist in the development of a more comprehensive threat assessment. Secretary Chertoff, speaking from his experience as a former federal prosecutor and judge, has noted that many organized crime cases were intelligence driven and that state and local police were best placed to discover anomalies in their communities that can lead to the prevention of violent acts.[14] Although the fusion process as outlined above goes beyond law enforcement or criminal intelligence, the counterterrorism role of state and local law enforcement has been outlined in numerous reports.[15] Those who agree with Secretary Chertoff are apt to argue that the 800,000 plus law enforcement officers across the country know their communities most intimately and, therefore, are best placed to function as the "eyes and ears" of an extended national security community. They have the experience to recognize what constitutes anomalous behavior in their areas of responsibility and can either stop it at the point of discovery (a more traditional law enforcement approach) or follow the anomaly or criminal behavior, either unilaterally or jointly with the Federal Bureau of Investigation (FBI), to extract the maximum intelligence value from the activity (a more intelligence-based approach).[16]

Numerous examples are cited by officials as demonstrating the counterterrorism role that state, local, and tribal governments and, by extension, fusion centers which have law enforcement as their core function, can play. Ambassador Thomas McNamara — the Program Manager for the Information Sharing Environment[17] — cited three examples at the First Annual National Fusion Center Conference. The first was a narcotics investigation conducted by federal, state, and local law enforcement that "...revealed a Canadian-based organization supplying precursor chemicals to Mexican methamphetamine producers was in fact a Hezbollah support cell." A second case involved a local law enforcement investigation in Torrance, California in which an individual engaged in a series of gas station robberies dropped his cell phone. The phone was exploited by law enforcement officers who "... uncovered a homegrown Jihadist cell planning a series of attacks." Another investigation into cigarette smuggling by a county sheriffs office "... uncovered a Hezbollah support cell operating in several states."[18] One additional incident often

---

[14] Ibid.

[15] See *When Terrorism Hits Home: How Prepared Are State and Local Law Enforcement* (RAND, 2004) and *State and Local Intelligence in the War on Terrorism* (RAND 2005). See also *The Impact of Terrorism on State Law Enforcement: Adjusting to New Role and Changing Conditions*, April 2005, The Council of State Governments and Eastern Kentucky University.

[16] At the Federal level, some have argued the FBI has shifted between these two approaches over time. See "FBI Alters Tactics in Fight Against Terrorists," in *Wall Street Journal*, May 23, 2007.

[17] The Information Sharing Environment was established pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), section 1016.

[18] See "Building a Trusted Partnership," Remarks of Ambassador Thomas McNamara at the (continued...)

cited case originated in Los Angeles, California where an investigation of a car theft ring led to the discovery of a domestic group supporting Chechen terrorists.[19]

One school of thought suggests that sound law enforcement alone can disrupt terrorist plots. This theory may be accurate as it pertains to individual terrorists or terrorist groups that are not particularly well-trained or resourced and, as a result, may be more aspirational than operational. However unsophisticated and low-tech these amateur extremist groups may be, their intent is hostile and their activities are, it could be argued, worthy of disruption, generally through law enforcement actions.[20] One important question regarding this theory is — are basic law enforcement tools, which demand a criminal predicate *prior to* the collection of intelligence, likely to only uncover less sophisticated terrorists and forms of terrorist activity?[21] Are current law enforcement methodologies, including those that are deemed "proactive," such as intelligence-led policing, effective tools for discovering the unknowns about potential terrorist activity in one's community, or are different approaches necessary?[22] It could be argued that sophisticated terrorist operatives may be so well-trained as to avoid any potential illegal activity that may undermine their inimical plots. These operatives may dissociate themselves from direct interaction with supporters who may engage in criminal acts. Do all terrorists or terrorist supporters within the United States engage in criminal activity? The answers to this question are arguable. If, however, the premise that sophisticated terrorists do not necessarily engage in criminal activity is accepted, is reactive and *ex post facto* collection of

---

[18] (...continued)
National Fusion Center Conference, Destin, Florida, March 6, 2007, p. 2.

[19] See "Criminal Intent: An L.A. Police Bust Shows New Tactics for Fighting Terror — Officers Use Local Laws to Arrest Small Offenders with High-Risk Potential — Foiling a Chechen 'Charity'," in *Wall Street Journal*, December 29, 2006, p. A1.

[20] See Daniel L. Byman, "The Rise of Low-Tech Terrorism," in *Washington Post*, May 6, 2007, p. B3. An example which may support Byman's argument is the recent arrest of a group of men accused of plotting to attack a military base in New Jersey (NJ). The would be terrorists were ultimately discovered because they took one of their terrorism training videos into a Circuit City store to be copied into DVD format. While the clerk's actions in calling the local police, who subsequently called NJ Office of Homeland Security and Preparedness, are laudable, one could question whether a well-trained terrorist operative would have engaged in such amateur behavior.

[21] Levels of sophistication in terrorist activity would include the extent to which terrorists have received training — and are experienced in — secure communications; clandestine movement of funds; spotting, assessment, and recruitment of suicide bombers to implement attacks; target selection (including political implications of various attacks); logistics and technical aspects of bomb-making and delivery, among other functions.

[22] Intelligence-Led Policing is defined as "...a collaborative enterprise based on improved intelligence operational and community-oriented policing and problem solving...information sharing must become a formal policy not an informal practice. Most important, intelligence must be contingent on quality analysis of data." See U.S. Department of Justice, Office of Justice Programs, *Intelligence-Led Policing: The New Intelligence Architecture*, September 2005.

intelligence sufficient to uncovering sophisticated terrorist plots?[23] Moreover, what are the limits of aggressive and pro-active intelligence collection by state, local and tribal security and law enforcement personnel?

Benefits of Fusion Being a Team Function. Secretary Chertoff has also stated that fusion centers are one of the most important tools that the community has to collect and connect the dots that can protect people and critical infrastructure. He was, however, cautious to stipulate that he views these centers as entities of the state and local governments that established them, and that the federal government had no intention of controlling the centers. According to Secretary Chertoff, the desired "end state" is as follows:

> Ultimately, what we want to do is not create a single [fusion center], but a network of [centers] all across the country, a network which is visible not only to us at the federal level, but as important, if not more important visible to each of you working in your own communities so you can leverage all the information gathered across the country to help you carry our your very important objectives.[24]

The Secretary's emphasis on the importance of fusion centers serving the state and local communities that largely "own" and operate them has been echoed by others.[25] A counter-argument for concentrating fusion resources at the sub-federal level suggests that state and local authorities may not have the necessary resources and experience to conduct the level of advanced and/or strategic analysis necessary for achieving true "fusion."

Potential Risks to Fusion Centers

There are several potential risks associated with fusion center development. One risk focuses on the hazards associated with creating fusion centers without the requisite philosophical and organizational changes necessary within the intelligence and law enforcement communities to sustain the work of the centers. The other risks

---

[23] For a description of criminal activity terrorists may engage in to support operational or logistical activities see CRS Report RL34014, *Terrorist Precursor Crimes: Issues and Options for Congress*, by Siobhan O'Neil.

[24] Derived from CRS transcription of Secretary Chertoff's Keynote Address to the first annual National Fusion Center Conference, March 6, 2007.

[25] For example, Charlie Allen, DHS Chief Intelligence Officer, has made numerous statements regarding the simultaneous benefits of fusion centers at both the state and local level, for example, Charlie Allen, "Assessment of Information Sharing Centers," Testimony before the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee of the House Homeland Security Committee, September 7, 2006, transcript provided by Federal News, available from [http://www.lexis.com], accessed on July 26, 2007. Kentucky officials took a similar view about how their center will benefit the state and its citizens, see Kentucky Justice and Public Safety Cabinet, "Governor Ernie Fletcher Unveils Intelligence Center to Help Federal, State Agencies Prevent and Track Criminal Activity," Press Release, October 11, 2006, available from [http://www.kentucky.gov/Newsroom/justice/pr1011a.htm], accessed on July 26, 2007.

focus on factors that could ultimately diminish political and popular support for fusion centers, and ultimately result in their demise or marginalized contribution to the national homeland security mission.

Potential Risk — Underlying Philosophy. Some might argue that the rise of state and regional fusion centers may have been premature — that is, the establishment of these entities in the absence of a common understanding of the underlying discipline. Creating a fusion center is a tangible action that seeks to enhance state and/or regional coordination and cooperation to prevent and mitigate, and in some cases, respond and recover from, homeland security threats. However, if fusion center development occurs devoid of a more fundamental transformation, is any real progress made? Is the country any safer or more prepared with fusion centers or have we created a false sense of security? Given recent terrorist activity overseas, including plots and activity in the United Kingdom, what should fusion centers do to recognize potential indicators of similar plots in the homeland? It could be argued that if information flow into fusion centers is limited, the quality of the information is questionable, and the center doesn't have personnel with the appropriate skill sets to understand the information, then the end result may not provide value. Furthermore, if fusion center constituent agencies don't buy into a common fusion and prevention philosophy that arguably needs to accompany fusion centers (i.e., responsibility for security, a proactive approach, and need for understanding their environment to discern potential threats) can fusion centers be effective?

It is also important to ask: If fusion centers offer some benefit, who are the beneficiaries? Are the benefits limited to the states and regions the fusion centers were largely designed to serve, given the centers were largely molded by the needs, politics, and resources of the given jurisdiction? Or, is there a "free-rider" benefit for the federal government and the nation as a whole? It could be argued that with little or no investment in state and/or regional fusion centers, the federal government stands to gain some benefit. If it is possible for state and regional fusion centers to serve state, local, regional, and national interests, what is an equitable division of responsibility, labor, and resources?

Another philosophical concern stems from the different conceptions of intelligence among the intelligence and law enforcement communities (see **Appendix A**). In the absence of a common understanding about what constitutes intelligence, fusion center development and progress may be impeded. Ultimately, without a common framework among disparate fusion centers and other homeland security agencies, it is possible that benefits of the their efforts will remain narrow, rather than having a national impact. While fusion center guidelines (discussed more in-depth below) represent a movement to provide fusion centers with a common framework, and were generally well-received by the centers, arguably, the Guidelines have the following limitations: (1) they are voluntary, (2) the philosophy outlined in them is generic and does not translate theory into practice, and (3) they are oriented toward the mechanics of fusion center establishment.

Potential Risk — Civil Liberties Concerns or Violations . The essence of fusion, as outlined above, is the integration and analysis of existing streams of information and intelligence for actionable public policy ends — be they

counterterrorism, broader counter-crime issues, or natural disaster response. Embedded in the fusion process is the assumption that the end product of the fusion process can lead to a more targeted collection of new intelligence, to include private sector data, which can help to prevent crime. It could be argued that through a more pro-active and targeted intelligence process, one that has as its starting point an intelligence gap, or unknown about a particular threat, it is possible that sophisticated criminal groups could be undermined. However, the potential fusion center use of private sector data, the adoption of a more proactive approach, and the collection of intelligence by fusion center staff and partners has led to questions about possible civil liberties abuses. Director of National Intelligence, Mike McConnell, acknowledges the difficulty of balancing effective intelligence efforts with civil liberties concerns, stating:

> The intelligence community has an obligation to better identify and counter threats to Americans while still safeguarding their privacy. But the task is [a] inherently a difficult one...[one] challenge is determining how and when it is appropriate to conduct surveillance on a group of Americans who are, say, influenced by al Qaeda's jihadist philosophy. On one level, they are U.S. citizens engaging in free speech and associating freely with one another. On another, they could be plotting terrorist attacks that could kill hundreds of people.[26]

Arguments against fusion centers often center around the idea that such centers are essentially pre-emptive law enforcement — that intelligence gathered in the absence of a criminal predicate is unlawfully gathered intelligence. The argument is that the further law enforcement, public safety and private sector representatives get away from a criminal predicate, the greater the chances that civil liberties may be violated. Furthermore, it could be argued that one of the risks to the fusion center concept is that individuals who do not necessarily have the appropriate law enforcement or broader intelligence training will engage in intelligence collection that is not supported by law.[27] The concern is to what extent, if at all, First Amendment protected activities may be jeopardized by fusion center activities. According to the American Civil Liberties Union (ACLU), "We're setting up essentially a domestic intelligence agency, and we're doing it without having a full debate about the risks to privacy and civil liberties."[28] Furthermore, the ACLU is also concerned with having DHS perform a coordinating role at the federal level with respect to these centers. "We are granting extraordinary powers to one agency,

---

[26] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs,* July/August 2007.

[27] Some might argue that the entire concept for fusion centers, particularly those aspects involving the incorporation of private sector data that may not be accurate or based on any criminal predicate is fundamentally flawed. If there is little legal recourse for citizens to challenge information related to them that resides in commercially available databases, and such information is included in fusion center operations, privacy rights and civil liberties could be undermined.

[28] See Shane Harris, "Issues and Ideas - Fusion Centers Raise a Fuss," in *National Journal*, February 10, 2007.

without adequate transparency or safeguards, that hasn't shown Congress that it's ready for the job."[29]

Most of the fusion center representatives interviewed for this report appeared to be aware of the need to be respectful of privacy and civil liberties as a result of 28 CFR Part 23, the Fusion Center Guidelines,[30] the *National Criminal Intelligence Sharing Plan* (NCISP),[31] DHS/Department of Justice (DOJ)-sponsored fusion center conferences, and DHS — provided Technical Assistance Training, as well as interactions with peer fusion centers. Several fusion centers had, or were in the process of creating, a governance board, to serve an oversight function, especially on civil liberty concerns. In one case, a fusion center cited concern for civil liberties as the reason it had specifically chosen a former judge to sit on its governing board. Many centers also claim to have privacy policies, a couple of which were reviewed by local ACLU or other civil liberties organization representatives.[32]

However, few of the centers had aggressive outreach programs to explain to the public the type of intelligence activities their centers could and could not engage in. There are exceptions; for example, one state fusion center works closely with the most active civil liberties organization in the state, provides the center's standard operating procedures to the public, and has appointed a state attorney general office representative to the center's governing board in order to pro-actively address civil liberties issues.[33] Another state center has brought in a nonprofit research and training organization to audit their operations, plans to invite civil liberties groups into the center to show its operations, and even stenciled the First Amendment and the following quote by Harry Truman on its walls:

> In a free country we punish men for the crimes they commit but never for the opinions they have.[34]

An official from a fusion center that advocated a proactive approach to civil liberties-related outreach warned colleagues of the dangers of civil liberties abuses, saying, "even the perception of abuse associated with a single center, will be devastating for us all."[35]

---

[29] Ibid.

[30] One of the prominent Fusion Center Guidelines recommends fusion centers "Develop, publish, and adhere to a privacy and civil rights policy." See U.S. Department of Homeland Security & U.S. Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, available from [http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf], accessed on May 31, 2007, p. 49.

[31] Available at [http://www.it.ojp.gov/topic.jsp?topic_id=93] (accessed June 5, 2007).

[32] Interview with state fusion center representative, April 23, 2007.

[33] Interview with state fusion center representative, May 1, 2007.

[34] Interview with state fusion center representative, May 17, 2007.

[35] Remarks by State Fusion Center Official, National Fusion Center Conference, CRS Notes, March 6, 2007.

Those centers not engaged in a proactive civil liberties outreach effort cited the lack of need and/or the lack of funds as impediments for undertaking such an effort. Several fusion centers suggested they did not need such a proactive outreach program on civil liberties because there had been no local complaints about civil liberties abuses. In a few cases, fusion centers had done targeted outreach to assure specific communities that the fusion center and other law enforcement agencies were not out to target them, but these programs did not reach a large audience. Others suggested that other state/local agencies were responsible for such programs (although most of them were described as general homeland security-related, rather than specific to concerns related to the fusion center). In several cases, fusion centers suggested they wanted to do a public relations campaign, but they didn't have the necessary funds.

While this report is not meant to provide an authoritative legal interpretation of related law, due to disparate state laws authorizing fusion center or criminal intelligence activities, for purposes of criminal intelligence systems, most fusion centers operate under federal regulations, in addition to any applicable state policies, laws or regulations.[36] At the federal level, the authorities which guide the FBI in collection of intelligence are the *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.*[37] At the state and local levels, if there is any analogue to the Attorney General's guidelines for multi-jurisdictional criminal intelligence systems, it is 28 Code of Federal Regulations (CFR) -(Judicial Administration), Chapter 1 (Department of Justice), Part 23 (criminal intelligence systems operating policies). Many centers cite 28 CFR, Part 23 as the guiding legal mechanism for their criminal intelligence operations. By its terms, 28 CFR, Part 23, applies to "all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, as amended." From the perspective of intelligence collection, the 28 CFR, Part 23 standard is reasonable suspicion. One of the operating principles of 28 CFR, Part 23 is that "A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[38] Further:

---

[36] See e.g. Burns Ind. Code Ann. §§5-2-4-1, 10-19-10-1 through 10-1-10-4; Va. Code Ann §§52-47, 44-146.22 note.

[37] The Guidelines stipulate three level of investigation into threats - threat assessments, preliminary investigation, and full field investigation; each level has certain legal thresholds and investigative tools attached to it. Depending on available information, these investigative tools and techniques range from non-intrusive (open source collection) to intrusive (electronic surveillance). The least intrusive of all level of investigation is the threat assessment, which allows the FBI to pro-actively "...use available information to identify terrorist threats and activities...when the FBI receives information or an allegation about possible terrorist activity, and the matter can be checked out promptly through relatively non-intrusive techniques." See U.S. Department of Justice, *Fact Sheet, Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*, November 3, 2003, pp. 2-3.

[38] See 28 CFR, Part 23, Section 23.20 (a) and (c) (Operating Principles).

> Reasonable Suspicion or Criminal Predicate is established when information exists which established sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individuals or organization is involved in a definable criminal activity or enterprise.[39]

The question of how to balance civil liberties with security remains an open issue Congress and the country often weighs. The balancing is, arguably, a moving target driven by the country's collective sense of security and safety. The nation cannot necessarily have absolute security, nor absolute liberty; a pendulum swings between relative amounts of each of these "public goods." The question, to which there is no definitive answer, raised here is how aggressive should fusion centers be in pro-actively collecting and analyzing intelligence that may go beyond that which may be entered into criminal intelligence systems that fall under federal law? Which entity at the federal level is auditing the activities of fusion centers to ensure civil liberties are not violated? Given that these centers are creations of state and local governments, should an entity of the federal government be the ultimate arbiter of civil liberties protection?

Potential Risk — Time. Some homeland security observers suggest that the rush to establish and enhance state fusion centers is a post-9/11 reaction and that over time some of the centers may dissolve. It could be argued that in the absence of another terrorist attack or catastrophic natural disaster, over the course of the next 5 to 10 years, state and regional fusion centers may be eliminated and/or replaced by regional fusion organizations. The state fusion regional representation organizations may be an entity to facilitate future center consolidation efforts. Issues that may lead to state and regional fusion center consolidation into regional organizations include:

- Perceived lack of need by state leaders;
- State and federal financial constraints;
- Duplication of effort without showing tangible products and services within a given center; and
- Reduction of risks to a given geographic location.

Alternatively, if there are additional terrorist attacks or natural disasters in the near future and fusion centers can demonstrate their tangible value by serving as proactive, analytic and/or operational information/intelligence hubs, it is plausible that substantial additional federal, state, and local funds may flow to these centers.

Potential Risk — Funding. A potentially time-related risk is the threat diminished or eliminated federal and/or state funding poses to fusion center development. If the United States is not the target of a successful terrorist attack, homeland security funding, arguably, may decrease. If overall federal funding levels for homeland security decrease, it is possible that there will be some level of decrease in Homeland Security Grant Program (HSGP)[40] funding. Such a decrease might

---

[39] Ibid.

[40] Homeland Security Grant Program is comprised of five interconnected grant programs: (continued...)

force states to re-prioritize funds for those programs deemed the most critical to their jurisdiction. Specific federal programs that fund and/or support fusion centers (i.e. DHS and FBI detailee programs) could potentially also suffer under funding cuts. It is unclear how fusion centers would fare in such a situation. It is likely that the fate of fusion centers would differ drastically from state to state, depending on a range of factors, to include, their level of maturity, buy-in from other agency partners, their resource needs, and noted successes, balanced with other critical issues and programs within the jurisdiction.

During research for this report, one fusion center official stated that if federal funding went away, his fusion center would continue to operate, albeit with less staff and possibly with a more limited scope. It could be argued in some states that fusion centers would not be able to continue long after federal dollars and support ceases to exist. Others might disagree, believing it is quite possible that many fusion centers would survive despite dwindling federal support. It is even possible that many fusion centers would survive even after drastic decline in state and local funding because states and localities would be in a difficult position to officially dismantle these centers.

Evolution of Fusion Center Concept

As previously mentioned, almost all state and regional fusion centers were created after the September 11th attacks. While the attacks were the direct impetus for the creation of most state and regional centers, the fusion center movement did not occur in a vacuum and can be best understood as a continuum of a mounting tide. Important influences include the increasing favor of the Intelligence-Led Policing model, among others; the perception that the High Intensity Drug Trafficking Area (HIDTA) Center structure was successfully enhancing coordination; rising agreement amongst Governors that each state should have a fusion center; and the support of the President and key federal homeland security entities, such as the Homeland Security Advisory Council (HSAC), and the Director of National Intelligence (DNI) — Information Sharing Environment Program Manager's Office.

Intelligence-Led Policing and Other Policing Models

In the decade prior to the attacks, the Intelligence-Led Policing (ILP) model[41] was gaining favor in the United States following the dramatic drop in crime in Kent,

---

[40] (...continued)
(1) State Homeland Security Program, (2) Urban Area Security Initiative (UASI), (3) the Law Enforcement Terrorism Prevention Program (LETPP), (4) the Metropolitan Medical Response System (MMRS), and (5) the Citizens Corp Program (CCP). See DHS, Office of Grants and Training, *FY 2007 Homeland Security Grant Program — Program Guidance and Application Kit*, January 2007, p. 1.

[41] Other policing models such as Community Oriented Policing and Problem Oriented Policing were also gaining momentum and popularity during this time - each model also relies heavily on intelligence and situational awareness, although less explicitly than Intelligence-Led Policing.

England, where it was originally developed, and the reported increase in use of the model in Europe and Asia.[42] The model, according to the Department of Justice's Bureau of Justice Assistance, is a

> collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving.... To implement intelligence-led policing, police organizations need to reevaluate their current policies and protocols. Intelligence must be incorporated into the planning process to reflect community problems and issues. Information sharing must become a policy, not an informal practice. Most important, intelligence must be contingent on quality analysis of data. The development of analytical techniques, training, and technical assistance needs to be supported.[43]

Additional law enforcement strategies, like Community-Oriented Policing (COP) and Problem-Oriented Policing (POP), which were becoming in vogue during the same period, also rely heavily on intelligence and situational awareness, although less explicitly than Intelligence-Led Policing.[44] These models highlighted the importance of intelligence and/or situational awareness in crafting proactive, preventative, and targeted law enforcement strategies. The focus of these models on both intelligence and the importance of a proactive stance are likely to have influenced the later support for fusion centers.[45]

HIDTA

The High Intensity Drug Trafficking Area (HIDTA) Center model also impacted the rise of state and regional fusion centers. Since 1990, 28 areas have been

---

[42] Three years after adopting this policing model, Kent experienced a 24% decrease in crime - US Department of Justice (DOJ), "Intelligence-Led Policing: The New Intelligence Architecture," *US Department of Justice Website*, September 2005, available from [http://www.ojp.usdoj.gov], accessed on May 18, 2007 - hereon known as DOJ, "Intelligence-Led Policing." Law enforcement agencies in Europe and Asia reportedly were increasingly adopting intelligence-led policing - PR Newswire Association, "International Spies And Analysts Define New Model For Intelligence: Global Intelligence Forum Brings Together Twenty-Three Countries Including Saudi Arabia, Japan, And Israel," *May 23, 1998, available from [http://www.lexis.com]*, accessed on May 21, 2007.

[43] DOJ, "Intelligence-Led Policing.," vii.

[44] Ibid., 10-11.

[45] It should be noted that many critics of the ILP and COP find the lack of a commonly adopted explicit definition of the terms leads to confusion. A report on ILP by the Australian national crime and criminal justice research agency found, "Although there is a growing literature on intelligence-led policing...it has been generally assumed that the term speaks for itself, and definitions are rare." It could be argued that these models are more intangible theories that are not easily translated into strategic actions. As a result, it could be argued that ILP, COP, and other policing models may mean very different things to different people and even when there is agreement, they are difficult to implement. Quote from Jerry H. Ratcliffe, "Intelligence-led Policing," *Australian Institute of Criminology, Trends & Issues*, No. 248, April 2003, available from [http://aic.gov.au/publications/tandi/ti248.pdf], accessed June 4, 2007.

designated as HIDTAs across the country.[46] HIDTAs are designed to be multi-agency entities that facilitate the coordination of law enforcement counterdrug efforts across all levels of government. Prior to 9/11, the benefits of collocation, coordination of resources, and information sharing across agencies was apparent to many in the law enforcement communities, and there were several states and regions that were looking to replicate the HIDTA model in their communities. In one case, a state had discussed creating a HIDTA-like center in the area of the state that was not serviced by the existing HIDTA prior to 9/11, however, the initiative lacked the political support to facilitate funding.[47] After the attacks, the proposal was revised and soon thereafter became that state's fusion center.[48] In several cases, post-9/11 state/regional fusion centers have been located with HIDTA centers, and in one case, organizationally linked with the local HIDTA — perhaps an indication of the importance of the HIDTA model influence on the fusion center movement.

Grassroots Support — Governors and Homeland Security Advisors

The growing focus on more intelligence-oriented policing models and the success of multi-agency law enforcement efforts, like the HIDTAs, combined with post-9/11 public demand and political support to create a strong movement toward including sub-federal law enforcement and non-traditional stakeholders in counterterrorism. However, unlike HIDTAs, which are largely federally funded and managed, this new movement was largely a grassroots movement with state and regional leaders leading the charge. Former Massachusetts Governor Mitt Romney is an advocate of the role states and locals would play, stating:

> Fundamentally, we recognize that we can't protect the homeland by just putting a cop out on the corner of the street. We have too many bridges, roadways, hospitals, schools, tunnels, trains. You just can't protect all of the possible terrorist targets. You have to find the bad guys before they carry out their bad acts. That requires intelligence. And the states and localities are going to finally have to be a major part of that.[49]

This appears to be a manifestation of a fundamental shift in thinking regarding responsibility for national security in which state and local officials are increasingly taking responsibility for traditionally conceptualized federal roles. This may have been the result of a belief that regardless of origin — a terrorist training camp in Afghanistan or a radicalized cell in Lackawanna, NY — state and local public officials are ultimately responsible for the safety of their citizens. Furthermore, there

---

[46] "The High-Intensity Drug Trafficking Area Program: An Overview," White House Website, available from [http://www.whitehousedrugpolicy.gov/hidta/overview.html], accessed on May 18, 2007.

[47] Interview with state fusion center official, May 4, 2007.

[48] Ibid.

[49] CNN American Morning, "Breaking News: Bin Laden Tape, Interview With Governor Mitt Romney," CNN Transcript, December 16, 2004, available from [http://www.lexis.com], accessed May 18, 2007.

was a strong sentiment among state and local officials and law enforcement agencies that the federal government had not provided enough of the right information and intelligence to enable them to potentially prevent a future attack or at least mitigate its impact and respond effectively.

Shift in Homeland Defense and Security Responsibility

Traditionally, national defense and security were the responsibility of the federal government. The Homeland Security Advisory Council (HSAC) acknowledged this reality when it addressed intelligence sharing in its 2005 report, which states:

> For the most part, terrorism-related information has traditionally been collected outside of the United States. Typically, the collection of this type of information was viewed as the responsibility of the intelligence community and, therefore, there was little to no involvement by State and local enforcement entities.[50]

It could also be argued the nature of post-Cold War, transnational, sub-state threats increasingly requires all levels of government, all levels of law enforcement and a wider spectrum of public and private officials to work together to protect the United States. This may be especially important given the possibility that:

> those wanting to commit acts of terrorism may live in our local communities and be engaged in criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories.[51]

Characteristics of State/Regional Fusion Centers

There appears to have been two waves of post-9/11 fusion center development: the first occurring in 2003, and the second wave of fusion centers that gained momentum in approximately 2005. Based on conversations with some fusion centers, this second wave gained momentum following the National Governor's Association (NGA) meeting in 2005. Indeed, the NGA published its 2006 survey of state homeland security advisors and found that "developing a state intelligence fusion center" ranked as their third priority.[52] The importance of fusion centers to "enhance states' ability to collect, analyze and disseminate intelligence [and] intelligence sharing among federal, state, and local government," was a priority in the previous survey NGA released in January 2005. Other catalysts include the

---

[50] U.S. Department of Homeland Security, Homeland Security Advisory Council, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion*, April 28, 2005, 2.

[51] Ibid.

[52] National Governor's Association (NGA), "2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships,"available from [http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf]; accessed on May 23, 2007, 3.

Homeland Security Advisory Council (HSAC)[53] meeting in March 2005, the preliminary conclusions of which included that:

> each state should establish an information center that serves as a 24/7 "all source," multi-disciplinary, information fusion center.[54]

Many fusion centers also stated that their elected leaders, law enforcement, and other officials realized that this was a national trend and recognized that the federal government was starting to provide funding to support existing centers. A defining moment in this realization appears to have been when the National Governors Association issued its 2007 "A Governor's Guide to Homeland Security," which identified intelligence fusion centers as one of 10 "key points" a new governor should examine in an effort to enhance their state's security. Intelligence fusion centers, according to the NGA, are:

> the focal point for information and intelligence sharing among local, state, and federal agencies from a variety of disciplines.[55]

The continued efforts of Global Justice Information Sharing Initiative (Global),[56] the establishment of the ISE, and the publication of the Fusion Center Guidelines, amongst other developments, also appear to have validated the growing fusion efforts at the state and local level. Furthermore, several fusion centers suggested Hurricane Katrina was influential in either solidifying their conviction that coordination of multiple stakeholder agencies via the fusion center was important for their state, and/or influencing their interest in an all-hazards approach.

Ownership/Stewardship

The overwhelming majority of the centers examined by the authors are state-wide in jurisdiction and are largely operated by the state police or state bureau/division of investigation. These state fusion centers are largely the outgrowth or expansion of an existing intelligence and/or analytical unit or division within the state's law enforcement agency. In many cases additional personnel, slightly expanded mission/scope, and additional resources were added to the existing intelligence unit infrastructure. As such, these state centers were more likely to stand up in a shorter period of time than those centers that regions established anew. As

---

[53] For more information on HSAC, see [http://www.whitehouse.gov/news/releases/2002/03/20020321-9.html], accessed May 21, 2007.

[54] On the other hand, however, there was a note in the meeting notes following this suggestion that read "to be further investigated by the Working Group," Homeland Security Advisory Council, Summary of Meeting Notes December 14, 2004, Dated March 7, 2005, available from [http://www.dhs.gov/xlibrary/assets/HSAC_MtgSummary_121404.pdf], accessed on May 21, 2007.

[55] NGA, A Governor's Guide to Homeland Security, 2007, available from [http://www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF], accessed on May 22, 2007, 8.

[56] The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee and advises the Attorney General on Justice information sharing and integration activities.

previously stated, due to their origins and development, some have referred to this type of state fusion center as "state police intelligence on steroids."

Less than 20% of fusion centers studied for this report were regional/local in jurisdiction. The majority of regional centers exist in Urban Area Security Initiative (UASI) regions, usually large cities with substantial populations and numerous critical infrastructure sites. The regional centers were more likely than state centers to have multiple agencies involved in their development and day-to-day operational management.

Legal Authority

The majority of fusion centers do not operate under a separate and fusion center-specific legal authority. Currently, the states legal authorities recognizing or establishing a fusion center range from nonexistent, to memorandums of agreements by the partnering agencies, and in one case a state statute which defines the center and its responsibilities. The majority of the existing fusion centers are not currently recognized by a governor's executive order or by state legislation — rather, as most centers are an outgrowth of the existing state law enforcement agency. As such, they tend to derive their authority from statutes that created those state police agencies or bureaus of investigation. Many of the fusion centers rely on internal policy documentation to demonstrate the establishment of the centers: policy memoranda signed by leaders of the state offices of homeland security or law enforcement organizations, Memoranda of Understanding (MOU) between agencies participating in the center, and/or internal center directives discussing the roles and responsibilities of the organization. In one case, prior to the issuance of an executive order, a regional center operated simply by partner agency consensus in the absence of specific legal authority.[57]

The DHS and DOJ-produced Fusion Center Guidelines[58] are silent on the issue of recommended authorities desired to support the establishment and continuing operation of a state fusion center. The lack of official state recognition of these centers could prove troubling for fusion centers in the future. If there is a reduction in future federal funding or moves to a cost-sharing model, federal grant deciding bodies may view those fusion centers with sustained in-state funding streams and/or a statutory recognition as more attractive candidates for continued federal funding.

Multiple Fusion Centers

In several states there are more than one fusion center. The number of fusion centers, as variously defined, within a single state ranges from two to eight. In some states, the fusion centers appear to work well together, or at least have taken steps to enhance their working relationship. In several states, they have worked to prevent the creation of multiple, non-integrated information silos by ensuring automatic

---

[57] Interview with state fusion center official, May 2, 2007.

[58] Department of Homeland Security and Department of Justice, *Fusion Center Guidelines*, August, 2006. [http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf].

electronic data sharing or using the same information management system. In at least two states, representatives from the fusion centers and/or it's managing agency sat on the governing board of the other center in the state. There was one case in which a regional fusion center worked to help secure more funding for the state center, which was having trouble getting homeland security grant funds due to the 80/20% mandated split for local and state governments[59] (this will be addressed in more depth later in the report). In other cases, there appeared to be friction when several fusion centers are operating (or are proposed for development) within a single state — some even appeared to be in competition with each other. Overall, the relationships between the multiple fusion centers within a single state haven't been long established and well tested. It has been reported that in November 2007, DHS Secretary Chertoff and Attorney General Mukasey sent a letter to each state governor asking for the designation of a single fusion center to interface with the federal government for purposes of sharing homeland security information.[60]

Mission/Scope

Given the fractured development of grassroots fusion centers around the country, and the broad nature of federal guidelines on the subject, fusion centers have significantly different roles and responsibilities. Some fusion centers are solely counterterrorism focused, while others have a broader mission. Some are prevention oriented, while others have a response and/or recovery role.

With regard to the ultimate purpose of state and regional fusion centers, the topic remains open to debate. In some cases the stated purpose of these centers has shifted in the few years they have been operating. Many of the "first-wave" centers, those created soon after 9/11, were initially solely focused on counterterrorism. Today, less than 15% of the fusion centers interviewed for this report described their mission as solely counterterrorism. In the last year, many counterterrorism-focused centers have expanded their mission to include all-crimes and/or all-hazards. For some this shift is official, for others it is defacto, reflected in the day to day operations of the center, but not in official documentation.

This shift towards an all-crimes and/or all-hazards focus can be explained by several factors: appearance of a national trend, need for local and non-law enforcement buy-in, and need for resources. First, leadership at several fusion centers interviewed for this report noted they believed the country was moving towards an all-crimes and/or all-hazards model and they felt they needed to move with the changing tide. Others suggested it was impossible to create "buy in" amongst local law enforcement agencies and other public sectors if a fusion center was solely focused on counterterrorism, as the center's partners often didn't feel threatened by terrorism, nor did they think their community would produce would-be terrorists. Rather, most police departments and public sector agencies are more concerned with issues such as gangs, narcotics, and street crime, which are more

---

[59] See CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, February 2, 2007.

[60] *Jason Miller, "States Must Designate Fusion Center to Work With Feds," Federal Computer Week, December 11, 2007.*

relevant to their communities. Lastly, one fusion center mentioned that having a wider purpose, that is all-crimes and/or all-hazards, allowed the fusion center to apply for a greater array of grants and draw on resources from more public agencies and individual partners.

All-Crimes. A little more than 40% of fusion centers interviewed for this report describe their center's mission as dealing with "all-crimes." There were shades of meaning in the definition of "all-crimes" across fusion centers. Some fusion centers were concerned with any crime, large or small, petty or violent. Such centers provided support to investigations into single criminal acts and larger criminal enterprises. Some centers, however, focused on large-scale, organized, and destabilizing crimes, to include the illicit drug trade, gangs, terrorism, and organized crime. One such center made the distinction that this approach was "homeland security focused," rather than all-crimes, which appears to recognize the potentially destabilizing impact the aforementioned crimes can have on the overall security of a community or region.

All-Hazards. A little more than 40% of fusion centers interviewed for this report describe their center as "all-hazards"as well as all-crimes. It appears as if all-hazards means different things to different people. The term itself appears to have come out of the Federal Emergency Management Agency (FEMA) work in the early 1980s to develop evacuation plans not only in response to nuclear attack, but to address all-hazards.[61] The all-hazards approach to preparedness and mitigation — two of the four interrelated emergency management actions (the other two being post-event, response and recovery) — soon became part of the federal government and FEMA's approach to emergency management. In many ways the concept has evolved from a preparedness focus to a more proactive stance.

After the September 11th attacks, the federal government continued to emphasize an all-hazards approach to preparedness. Indeed, the December 2003 Homeland Security Preparedness Directive (HSPD) No. 8 encourages an all-hazards approach to homeland security preparedness and specifically defines "all-hazards preparedness" as "preparedness for domestic terrorist attacks, major disasters, and other emergencies."[62] However, the focus of the term seems to have shifted with the help of the fusion center movement, as some fusion centers appear to have adopted an all-hazards mission with a more proactive, prevention-focused stance.

---

[61] "Intimations of Mortality," The Economist, November 26, 1983, available from [http://www.lexis.com], accessed on June 4, 2007 & see U.S. Federal Emergency Management Agency, *Guide for All-Hazard Emergency Operations Planning*, September 1996, available from [http://www.fema.gov/pdf/plan/slg101.pdf], accessed on June 4, 2007, which states, "flexible enough for use in all emergencies — including unforeseen events — provides a community with an emergency management "bottom line." From there, a community can proceed confidently with long-term *mitigation* efforts directed at specific hazards. Or, it can devote more resources to risk-based *preparedness* measures (e.g., specialized training, equipment, and planning). Whatever the initiative, an all-hazard EOP helps the community start from a position of relative security."

[62] "Homeland Security Presidential Directive/HSPD-8," December 17, 2003, available from [http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html], accessed on May 18, 2007.

Moreover, there are some indications that different fusion centers viewed "all-hazards" as pertaining to either their data streams, agency partners, or the center's role. For some, all-hazards suggests the fusion center is receiving and reviewing streams of incoming information (i.e., intelligence and information) from agencies dealing with all-hazards, to include law enforcement, fire departments, emergency management, public health, etc. To others, all hazards means that representatives from the aforementioned array of public sectors are represented in the center and/or considered partners to its mission. At some centers, all-hazards denotes the entity's mission and scope — meaning the fusion center is responsible for preventing and help mitigating both man-made events and natural disasters. For others, "all-hazards" indicates both a pre-event prevention role as well as a post-event response, and possibly recovery, role.

Several fusion center officials that described their center as having an all-hazards focus mentioned the influence of Hurricane Katrina on their center's development. In most cases, the fusion centers with an all-hazards mission sought to facilitate intelligence/information sharing and analysis pre-event (whether man-made or natural disaster), but unlike some entirely prevention-oriented, all-crimes- or counterterrorism-focused centers, also facilitated situational awareness post-event (again for both man-made or natural disaster). In most cases, all-hazards-oriented fusion centers sought to act as a force multiplier and support structure for existing Emergency Operations Centers (EOCs), which remain responsible for coordinating the response to large-scale incidents and disasters.

Operational v. Analytical

The majority of fusion centers interviewed for this report serve a solely, or at least primarily, analytic role. These centers operate a support function for operations and investigations, but are not directly engaged in such activities, although there were some exceptions. Those centers that are more operational in nature tended to be either largely "owned" and operated by a single state police/bureau of investigations agency, and/or predominately staffed by sworn law enforcement personnel (as compared to more analyst-heavy fusion centers).

The fusion center leadership of state-wide centers, which were largely "owned" by one state agency, tended to have a more direct relationship with the "boots on the ground." These centers operated under the same parent agency, usually a state police or investigation agency, making it easier to have direct access to both investigators and their information/intelligence collection efforts. Regional and more-multi-agency "owned" centers appeared unable, largely due to chain of command issues, to directly task their partner agencies' staffs. The operational activities of these centers included responding to incident scenes, running/assisting with investigations, and tasking collectors. In one case, a fusion center provided an operational support unit to assist local law enforcement with investigations where it lacked appropriate equipment and/or personnel.[63]

---

[63] Interview with state fusion center official, May 4, 2007.

Prevention and/or Response

Most fusion centers fulfill both prevention and response functions, with a bias toward prevention. Many states that have a separate emergency management organization can direct greater attention toward prevention.

Prevention. The overwhelming majority of fusion center officials interviewed for this report saw their centers as primarily prevention-oriented entities. In order to prevent, as well as mitigate, a variety of threats, fusion centers work to enhance information sharing, conduct threat assessments and analysis, and support and/or facilitate preparedness efforts. To those ends, most fusion centers acted as:

- intelligence/information relay centers;
- collocation centers for personnel from various agencies (often with access to their agencies' databases);
- facilitators of coordination on a variety of projects;
- analytic centers; and
- case support centers.

For example, some centers operated largely as filtering stations — sifting through many finished information and intelligence products from federal agencies, other state fusion centers, and state and local law enforcement agencies to identify relevant information for the center's jurisdiction, which would be distributed to customer agencies in the region. Others added analytic value to existing products by supplementing local information or explicitly highlighting local connections to the larger trends. Some fusion centers check the variety of databases they and their partner agencies have access to in response to inquires from local police departments, as the result of a private citizen tip relating to a suspicious incident, or as a result of information gleaned from another information product. Sometimes fusion centers provide case support to law enforcement agencies (at all levels of government). As a general trend, it appears as if all of the fusion centers interviewed for this paper are involved in at least one step of the intelligence cycle, but none appears to be involved in all steps of the cycle.

Response. In most states, there is an emergency management agency and/or operation center that is responsible for response activities to both man-made and natural disasters.[64] However, in numerous cases, the fusion center is described as playing a situational awareness role to support the emergency operations center (EOC) during events. Some fusion centers said they had a reserved seat at the EOC that they could access during events. In a few cases, fusion centers had a more active role: at least two have sent analysts to the command posts at both high profile events (i.e. pro golf tournaments) and relevant emergencies (i.e. a fire or an explosion) to relay information back to the fusion center.

---

[64] According to NGA survey data, "100 percent of respondents have established a statewide emergency operations center" — based on 2004 survey for 2005 report, with 38 of the 55 U.S. states and territories responding, the survey achieved a 69 percent response rate - *Homeland Security in the States: Much Progress, Much Work*, January 24, 2005, available from [http://www.nga.org/cda/files/0502HOMESEC.pdf], accessed on May 23, 2007.

Proactive v. Reactive

As previously stated, the overwhelming majority of fusion centers reviewed for this report were described by their leadership as being primarily prevention focused. In order to be successful in preventing (and mitigating) threats, fusion center officials across the county frequently advocate the proactive stance their centers have adopted. Many fusion centers state their proactive orientation marks a departure from traditional policing, which is often reactive, post-event, and prosecution focused. However, research indicates that while fusion centers want to become more proactive, many continue to follow a reactive model.

Most fusion centers respond to incoming requests, suspicious activity reports, and/or finished information/intelligence products. This approach largely relies on data points or analysis that are already identified as potentially problematic. As mentioned above, it could be argued that this approach will only identify unsophisticated criminals and terrorists. The 2007 Fort Dix plot[65] may serve as a good example — would law enforcement have ever become aware of this plot if the would-be perpetrators hadn't taken their jihad video to a video store to have it copied? While state homeland security and law enforcement officials appear to have reacted quickly and passed the information to the FBI, would they have ever been able to find would-be terrorists within their midst if those individuals avoided activities, criminal or otherwise, that might bring to light their plot?

It is unclear if a single fusion center has successfully adopted a truly proactive prevention approach to information analysis and sharing. No state and its local jurisdictions appear to have fully adopted the intelligence cycle. While some states have seen limited success in integrating federal intelligence community analysis into their fusion centers, research indicates most continue to struggle with developing a "true fusion process" which includes value added analysis of broad streams of intelligence, identification of gaps, and fulfillment of those gaps, to prevent criminal and terrorist acts.

Access to Information/Intelligence

An important consideration when assessing the maturity of fusion center information sharing and analysis efforts is the centers' access to and quality of relevant information and intelligence. Following the September 11th attacks, there was an outcry about the failure of information sharing between the federal intelligence and law enforcement communities and state and local officials. The 9/11 Commission concluded, "The biggest impediment to all-source analysis — to a greater likelihood of connecting the dots — is the human or systemic resistence to sharing information."[66] As some homeland security observers have noted those who do not share information outside their agency may use the classification barrier (not

---

[65] For more information see DOJ, "Six Individuals Charged with Plotting to Murder U.S. Soldiers at New Jersey Military Base," Press Release, May 8, 2007, available from [http://newark.fbi.gov/dojpressrel/2007/nk050807.htm], accessed on July 26, 2007.

[66] *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, p. 416.

having appropriate clearances) or the reciprocity challenge associated with security clearances (having a clearance sponsored by an agency other than the one that owned the information) as an excuse for failing to probatively share information. This was especially true with regards to vertical information sharing - sharing between federal agencies and sub-federal entities, like state and local law enforcement and other first responders.

Clearances. In the nearly six years since the attacks, it appears as if federal intelligence agencies have made a concerted effort to provide clearances to numerous state and local personnel. Almost all fusion centers studied for this report had multiple personnel with security clearances, although there were a couple of exceptions that had few if any cleared personnel. On average, fusion centers appear to have 14 staff with Secret clearances,[67] which is not insignificant considering the average staff size of the fusion centers interviewed for this report was approximately 27 full-time persons.[68] Clearances for state and local personnel were not restricted to Secret-level clearances, but also included some Top Secret (approximately 6 persons on average) and Top Secret-Secure Compartmentalized Information (SCI) (approximately one person on average) clearances as well.[69] In some cases federal detailees to the centers held the highest level clearances, in other cases, state, and local officials assigned to the center held TS/SCI clearances. It is important to note that discussions with fusion center officials suggest there is a lag between obtaining clearances and obtaining the necessary equipment for receiving and storing classified intelligence.

It appears the FBI provided most of the initial security clearances for state and local authorities following September 11th. According to the FBI, as of August 2005, 6,011 such clearances have been authorized since the program began in 2002.[70] However, based on interviews with fusion centers, that appears to be changing. Fusion center representatives claimed that in recent months DHS has increasingly conducted security clearances for state and local personnel at fusion centers. Fusion centers claimed that the DHS process has improved to the point that it was faster than the FBI's. In a few cases, fusion centers reported turning to DHS after local FBI leadership no longer offered to clear state and locals in their fusion center. Others

---

[67] For information on the various security clearances mentioned in this report see FBI, "Security Clearance Process for State and Local Law Enforcement," available from [http://www.fbi.gov/clearance/securityclearance.htm], accessed on July 27, 2007, and Derrick Dortch, "Getting a Security Clearance," The Washington Post, June 25, 2004, [http://www.washingtonpost.com/ac2/wp-dyn/A52768-2003Feb10?language=printer], accessed on June 27, 2007.

[68] For the purposes of this report, the authors attempted to focus on full-time personnel with clearances, although in some cases fusion centers have a large number of cleared part-time personnel.

[69] It should be noted that in some cases those individuals with Top Secret and Top Secret SCI clearances are actually federal detailees assigned to the center - however, although that may impact what information is shared and when is shared, it does represent the capability to receive highly classified information in the fusion center.

[70] Kevin Johnson, "FBI Gets Local Police in the Loop," *USA Today*, August 2, 2005, News Section, 3A.

suggested the FBI only provided high-end (Top Secret, TS SCI) clearances, while DHS conducted investigations for Secret clearances. Regardless of who is sponsoring security clearances for non-federal government personnel, issues remain regarding reciprocity among agencies in recognizing another's clearance which at times hinders an individual from accessing facilities and computer systems.

Classified Systems Access. In the past few years, state and local authorities have received increased and enhanced access to classified information systems. This appears to be largely facilitated by the proliferation of systems designed for state and local law enforcement and other public sector use, and due to increased collocation with federal agencies, and, as previously mentioned, a growing number of security clearances for state/local officials. DHS created HSIN, HSIN-Secret, and the Homeland Security Data Network (HSDN)[71] as portals to facilitate information sharing with and among state and local agencies, including at the classified level. Reportedly, DHS is considering replacing or upgrading the HSIN with a more efficient system for sharing homeland security information with state and local entities.[72]

In addition to the significant number of cleared state and local personnel at the fusion centers, fusion center collocation with federal agencies has also increased state/local access to threat intelligence and information. However, often that access was indirect (i.e. a federal official may need to access the information on behalf of state and local fusion center staff). For example, state/regional fusion centers collocated with the FBI's Joint Terrorism Task Force (JTTF) or Field Intelligence Group (FIG)[73] often have indirect, and sometimes direct, access to FBI information systems and/or the other systems housed in the facility's Sensitive

---

[71] HSIN-Intel is a portal DHS uses "primarily to disseminate current homeland security intelligence information and integrated intelligence assessments derived from both DHS and Intelligence community sources" to both law enforcement, first responders, and private sector homeland security partners. According to DHS officials, HSIN-Secret (HSIN-S) is the portal through which the Department"provides intelligence products up to the collateral SECRET classification level to our State and local partners..." HSDN is "analogous to the Department of Defense's Secret Internet Protocol Network (SIPRNET)." Charles E. Allen, "The Homeland Security Information Network: An Update on DHS Information Sharing Efforts," Statement for the Record before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, September 13, 2006, 5, 6, 7, respectively.

[72] *Spencer S. Hsu and Robert O'Harrow Jr., "DHS to Replace 'Duplicative' Anti-Terrorism Data Network," The Washington Post, January 17, 2008.*

[73] The purpose of the Field Intelligence Groups (FIG) as described by the FBI is to "manage and coordinate intelligence functions in the field. The FIGs are the mechanism through which the FBI contributes to regional and local perspectives on a variety of issues, including the receipt of and action on integrated investigative and intelligence requirements. In addition, FIGs provide the intelligence link to the Joint Terrorism Task Forces (JTTF), Fusion Centers, FBIHQ, and other intelligence community agencies. FIGs are staffed by intelligence analysts (IAs), special agents (SAs), language analysts (LAs), and surveillance specialists." John S. Pistole, Statement before the Senate Select Committee on Intelligence, January 25, 2007, available from [http://www.fbi.gov/congress/congress07/pistole012507.htm], accessed on June 27, 2007.

Compartmentalized Information Facility (SCIF).[74] Fusion centers that are not collocated, but that have federal agency detailees often have indirect access through those representatives. There are several fusion centers who have built, or are in the process of building, their own SCIF or secure room in order to have direct access to such systems.

Responsibility to Share Replaces Need to Know. The support within the federal IC and law enforcement agencies to share sensitive information with state and local law enforcement, fusion centers, and other public sector entities appears to have increased in recent years. Moving from a "need to know" rule to a "responsibility to share" rule[75] for information sharing and addressing the security designation and handling restrictions that act as barriers to effective information sharing appears to be a priority for the DNI's office, as is evident by the efforts of the Program Manager for the Information Sharing Environment (PM-ISE or ISE). However, it could be questioned whether the PM-ISE has authorities commensurate with the office's responsibilities to implement its initiatives across all levels of government.[76]

Numerous fusion centers officials claim that although their center receives a substantial amount of information from federal agencies, they never seem to get the "right information"[77] or receive it in an efficient manner. According to many state fusion center leaders, often pertinent threat intelligence must be requested by fusion centers, rather than federal agencies being proactive in providing it. The obvious difficulty arises regarding the inability to request relevant threat information that is unknown to members of the fusion center. The 9/11 Commission criticized the lack of incentives to share information and penalties for those who didn't share within the Intelligence Community. Even if federal IC agencies have instituted incentives and penalties for information/intelligence sharing, it is unclear if these requirements would apply to vertical sharing with state and local authorities, as well as the private sector counterparts and what mechanisms might be in place to assess effectiveness.

---

[74] It should be noted that the terms SCIF and secure room are often incorrectly used interchangeably to describe a separate office within a facility. A SCIF, according to the National Security Agency, is "an accredited area, room, group of rooms, buildings, or installation where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed." See NSA Website, available from [http://www.nsa.gov/business/busin00010.cfm], accessed on June 19, 2007. By contrast, a secure room is an office that has simple locking devices in place to control the flow of personnel into the area. A secure room is not built to the same structural specifications as that of a SCIF and can only store sensitive unclassified information.

[75] It is recognized that, notwithstanding a renewed effort to enhance information sharing, there remains a need to protect intelligence sources and methods.

[76] The responsibilities and authorities of the PM-ISE are outlined in P.L. 108-458, Section 1016.

[77] As mentioned above, this could be a perception problem amongst state and local personnel unfamiliar with the limits of national intelligence and/or an issue related to extent to which federal products are tailored to state and local needs. For more information, CRS Report RL34061, *Intelligence and Information-Sharing Elements of S. 4 and H.R. 1*, June 26, 2007, by Todd Masse.

Both H.R. 1 and S. 4, two bills pending before Congress, address enhanced information sharing mechanisms, including monetary and non-monetary awards to federal employees as incentives for information sharing.[78]

Information/Intelligence Sharing and Management

By all accounts information sharing between federal and sub-federal agencies has improved since the September 11th attacks. However, according to some fusion officials it appears that information sharing from the federal government to the state and local fusion centers continues to be a largely reactive, especially when it comes to information state and local officials believe is relevant to their jurisdiction. Several fusion center officials remarked that they receive such intelligence and/or information when they request it, which is an improvement over pre-9/11 situation, however according to fusion center officials, federal agencies are still not proactive in reaching out to state and regional fusion centers, sometimes even when a connection to that locality is apparent in an analytic product. Other fusion centers cited a lack of feedback when the fusion center or one of its state/local partners provides information up to the federal government.

State/Locally-Administered Systems. Research indicates that there may be a misconception that all states and regions are operating sophisticated intelligence management systems that have access to all databases available within their jurisdiction. Not every state has a state-wide intelligence system, in fact many don't. Such systems are expensive and potentially problematic in getting all agencies with homeland security-related missions to adopt a particular system. Even states that have such a system, often don't have access to all the data pools outsiders believe they do. For example, one center that is more mature than many of its counterparts reported having access to only 30% of the law enforcement data in the state — and that was good compared to other respondent fusion centers.[79] One state is preparing to go online with a statewide database that will have access to 92% of law enforcement records (state and local), but this is the exception rather than the rule.[80]

Access to Private Sector Systems. There is also a misconception that fusion centers, and the information management systems that some of them manage, have access to vast amounts of private sector data. This is largely unfounded. Even within fusion centers that have long established relationships with private sector organizations and individual companies, as some do, fusion centers do not typically appear to have access to their data. The flow of information from the private sector to fusion centers is largely sporadic, event driven, and manually facilitated. It does not appear that these databases are directly linked together. In general, the private sector seems very wary of that level of sharing — concerned with lack of government

---

[78] See Tile VII, section 723 of H.R. 1 RFS, Implementing the 9/11 Commission Recommendations Act of 2007; and Title I, section 114, of S. 4.ES, "Improving America's Security Act of 2007."

[79] Interview with state fusion center official, April 24, 2007.

[80] Interview with state fusion center official, May 7, 2007.

safeguards, industrial espionage, exposing weaknesses to competitors, as well as privacy and civil liberties concerns.

Lack of Interoperability of Systems. There are areas of concern related to these information management systems, specifically that there is a lack of coordination regarding the adoption of such systems nationally. In many cases, state-wide intelligence systems cannot work in conjunction with other systems within the state or regionally. Despite federal efforts to promote the use of Extensible Markup Language (XML) as the standard format across levels of government for justice and public safety information management systems,[81] fusion centers and states continue to purchase systems that operate using proprietary language and that cannot "speak" to other systems without additional equipment and costs. This may be due to the lack of mandatory guidance on this issue and other technology-related concerns. Currently, all guidance on this is voluntary.

Plethora of Federally-Sponsored Systems. In addition to funding concerns, the most consistent and constant issue raised by fusion center officials relates to the plethora of competing federal information sharing systems. The fusion centers interviewed for this report cited numerous sites operated by federal agencies that they needed to check in order to receive information from the federal law enforcement and intelligence communities, including, but not limited to, the HSIN and its sister systems HSIN-Secret and HSDN, Law Enforcement Online (LEO), Federal Protective Service (FPS) portal, Regional Information Sharing Systems (RISS), among others.

Respondent fusion center officials remarked that their staff could spend all day, every day reviewing all the information posted on these systems, and still not be confident they had seen all relevant and/or unique data. Often information is duplicated on several sites, but because of the occasional situation when it is not, fusion center officials believe they need to check them all. One official found the message from Washington regarding efforts to streamline dissemination channels contradictory with the continued promotion of individual agency's "pet projects" at the state and local level. In addition, fusion center officials found the systems' usability and security lacking. This problem affects not only how fusion centers receive information, but how they pass it to federal agencies. In several cases, it appeared as if information flow to a particular federal agency was severely impeded because the fusion center resisted using the system/portal run by the agency and did not have personal contacts to send information directly.

Classified Systems. Several fusion center officials mentioned problems related to the different requirements federal agencies have for creating secure spaces to house their classified information systems. The lack of reciprocity for such spaces and the lack of coordination between federal agencies likely results in increased costs for fusion centers. The construction of secure spaces needed to house classified intelligence systems can reportedly cost "two to 10 times the cost of conventional

---

[81] DOJ, Global JXDM User Guide: Building Exchange Content Using the Global JXDM: A User Guide for Practitioners and Developers, available from [http://it.ojp.gov/topic.jsp?topic_id=201], accessed on June 1, 2007.

office space, depending on features required."[82] Construction companies estimate that the cost of building a SCIF in an existing state/local facility can cost $200-$500 per square foot, and sometimes more depending on the requirements of the federal sponsoring agency.[83] Several fusion centers interviewed for this report mentioned estimated costs between $75,000-$100,000 to build each secure space at their respective centers. In a few cases, fusion centers mentioned they had been advised they would need more than one such space because individual federal agencies had different security requirements for their own systems. One such center that is moving to a new space was told they needed to create three different secure spaces to house different federal information systems — a cost that would be largely, if not entirely, borne by the center.[84]

Over-classification and Excessive Number of Security/Handling Instructions. Systematic over-classification was identified by the 9/11 Commission Report as preventing critical intelligence from reaching law enforcement, state officials and infrastructure operators.[85] It could be argued that the federal government has been slow to address the over-classification of intelligence, and the culture of "ownership" over intelligence products generated by particular federal intelligence or law enforcement agencies continues to be an obstacle to information sharing.[86] In addition, there is a serious lack of standardization regarding classification designations and dissemination guidelines.

Sensitive But Unclassified (SBU). Moreover, it has been argued that the federal government uses a large number of distinct security designations and a variety of handling instructions that make using classified information unnecessarily confusing and onerous. A 2006 Government Accountability Office (GAO) study found federal agencies involved with terrorism-related intelligence currently use "a total of 56 different designations for information they determined to be sensitive but unclassified, and agencies that account for a large percentage of the homeland security budget reported using most of these designations."[87] More than half of the agencies involved in the study reported encountering difficulties sharing sensitive but

---

[82] Barnaby Wickham, "BRAC Realignment Brings No Surprises to Baltimore Real Estate Executives," The Daily Record (Baltimore, MD), September 7, 2005, available from [http://www.lexis.com], accessed on June 5, 2007.

[83] Phone Interview with construction company engaged in SCIF construction, June 12, 2007.

[84] Interview with regional fusion center, May 3, 2007.

[85] See National Commission of Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, pp. 417-418.

[86] See Matthew M. Johnson, "Local Counterterrorism Efforts Handicapped by Intelligence-Sharing Woes," *CQ Homeland Security - Intelligence*, June 29, 2007.

[87] US Government Accountability Office (GAO), Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-related and Sensitive but Unclassified Information, (Washington DC: GAO, 2006), 21.

unclassified information.[88] This is certainly echoed by state and local law enforcement agencies, which found the "multiplicity of designations and definitions not only causes confusion but leads to an alternating feast or famine of information."[89] In addition, "lack of clarity on dissemination rules and lack of common standards for controlling sensitive but unclassified information, often overwhelm end users with the same or similar information from multiple sources."[90] GAO concluded that, without standardization for security designations, guidance and monitoring, there is a probability that "the designation will be misapplied, potentially restricting material unnecessarily or resulting in the dissemination of information that should be restricted."[91]

One PM-ISE effort that may ameliorate this issue is the Controlled Unclassified Initiative (CUI) which is seeking to reduce the number of SBU designations from over 100 to three, with clear instructions for security, handling, and dissemination.[92] This initiative appears to still be in the development stage.

Over-classification. Congress and the Administration have acted to address over-classification through the IRTPA which required the President within 270 days of the enactment of IRTPA 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.[93]

To date, it appears that no such guideline has been issued[94] and due to continued over-classification, it may be that fusion centers, as well as other pertinent SLT officials, may not receive all the relevant threat information they need. Before IRTPA, the 9/11 Commission also addressed the issue of over-classification in its final report. The report proposes that

> when a[n] [intelligence] report is first created, its data be separated from the sources and methods by which they are obtained. The report should begin with

---

[88] Ibid., p. 21.

[89] Ibid., p. 25

[90] Ibid.

[91] Ibid., p. 21.

[92] See *Federal Information at the Fusion Center: Rules of the Road*, an ISE presentation delivered at the National Fusion Center Conference, March 6, 2007. See also Ambassador Ted McNamara, Statement for the Record submitted to the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, April 26, 2007, available from [http://www.ise.gov/docs/HHSC-20070426-%20McNamara%20Testimony.pdf], accessed on June 19, 2007, 5-6.

[93] Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458 (SEC. 1016.(d)1).

[94] The PM-ISE *Implementation Plan* (November 2006, Table, ES-1, p. xvii) provides for two requirements and five guidelines, none of which directly address over-classification.

> the information in its most shareable, but still meaningful, form. Therefore the maximum number of recipients can access some form of that information. If knowledge of further details becomes important, any user can query further, with access granted or denied according to the rules set for the network — and with queries leaving an audit trail in order to determine who accessed the information.[95]

The argument that security designations are often necessary due to sensitive sources and methods, which prevents intelligence from reaching many SLT officials, may be overstated. In many cases, the intelligence may have even been culled from open source information. In addition, the majority of fusion center officials interviewed for this report were near emphatic that they were not concerned with sources and methods. Rather, fusion center officials wanted to know if the originating agency had deemed the threat credible and if the threat had been corroborated.

Funding: A State Perspective

While not mandated by federal law or executive order, many federal government agencies recognize the utility of state created fusion centers. As such, over the past two years the federal government has provided financial support to the fusion centers with the states continuing to pay for approximately 80% of fusion center budgets.[96] While state leadership has expressed appreciation for this funding others have questioned the effectiveness of federal government support to state fusion centers.[97] Other state leaders are concerned that the desire for additional federal funding and direction may be problematic as they are concerned that the greater support provided by the federal government will lead to prescriptive requirements levied on the fusion centers.[98]

According to FY2007 homeland security grant guidance, the State Homeland Security Program, Urban Area Security Initiative (UASI) grant program, and Law Enforcement Terrorism Prevention (LETTP) Program, and the Metropolitan Medical Response System (MMRS) grant program (the four of which comprise the overwhelming majority of all Homeland Security Grant Program (HSGP) funding streams, and the majority of all homeland security-related grants administered by

---

[95] National Commission of Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, Authorized Edition (New York: WW Norton & Company, 2004), 417-418.

[96] Numerical assessment derived from discussion with fusion center leaders detailing the approximate funds received to date from the federal government.

[97] Comments by fusion center leadership during the survey interviews noted that while the funding from the federal government was appreciated and needed to assist in establishing the center, the lack of strategy and direction accompanying the support left many centers confused regarding its role in homeland security as well as the federal strategy for information sharing.

[98] Comment by fusion center leader during CRS hosted fusion center discussion, May 31, 2007.

DHS[99]), require that at least 80% of all funds be passed to local jurisdictions.[100] This policy was cited continually by fusion center officials as a major hurdle in channeling the homeland security funds toward state-wide fusion center efforts. Several also cited the required spending split as leading to the creation of regional fusion centers within states that already had a state-wide center operating. These requirements have been used in several previous grant cycles.[101]

Much like the diverse missions of fusion centers, state and federal funding and programmatic support to the nation's fusion centers also varies greatly. As noted earlier in the report, to date the nation's fusion centers have largely been paid for with state funds. Some of the surveyed fusion centers did not receive state or federal start-up funds and were established by simply combining and renaming existing state and/or local public safety-related agencies into a state fusion center.

Annual budgets for the fusion centers studied for this report appear to range from the tens of thousands to several million (with one outlier at over $15 million). Similarly, the sources of funding differed significantly from center to center — as stated, some were entirely dependent on diverting funds from existing state and/or local funding streams, while others were largely funded by federal grants. Federal funding ranged from 0%-100% of fusion center budgets, with the average and median percentage of federal funding at approximately 31% and 21%, respectively. Thus, it appears that on the whole, fusion centers are predominately state and locally funded.

Staffing

In general, the fusion centers studied for this report remain largely law enforcement oriented entities. That said, centers appear to be increasingly bolstering their non-sworn officer ranks and reaching out to non-law enforcement homeland security partners.

Staffing Levels. Staffing levels at fusion centers that are fully operational range from 3 to nearly 250 full-time personnel, with the average number of full time staff at approximately 27 persons. Part time personnel ranged from 0 to over 100, with the average number of part time staff at fusion centers running far lower. Federal representation at the fusion centers in question is small percentage-wise, but can have a big impact on the center itself. Such participation can provide access to additional information streams and help facilitate the security clearance process, as

---

[99] The only HSGP program that does not is Citizen Corps. Grant allocations used to determine this assessment were provided by the Department of Homeland Security in phone calls on June 21 & 26, 2007.

[100] [U.S. Department of Homeland Security, FY2007 Homeland Security Grant Program: Program Guidance and Application Kit, January 2007, available from [http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_guidance.pdf], accessed on June 19, 2007, 39-40.

[101] For example, FY2003 and FY2004 grant guidance documentation, [http://www.dhs.gov/xnews/releases/press_release_0274.shtm] and [http://www.dhs.gov/xlibrary/assets/First_Responder_Press.doc], accessed June 19, 2007.

well as impact the overall relationship between the federal sponsor agency and the fusion center.

Law Enforcement Personnel. In general, law enforcement personnel are the dominant participants in the fusion centers studied in this report. Furthermore, the majority of sworn officers detailed to fusion efforts are from state police agencies and state bureaus of investigation, rather than local departments. Some may argue this is natural given the majority of fusion centers are state-wide entities that grew out of state police/bureau of investigation intelligence/analysis units. Of the local law enforcement agencies represented, the overwhelming majority are from the largest local police departments in the country, which have more resources, and in some cases, intelligence units (which are somewhat rare in local police departments as will be discussed below).

While in general, law enforcement and public safety officials have more prior experience with intelligence then the other non-law enforcement public sector entities that are increasingly involved in fusion centers, it is important not to overstate law enforcement experience and/or resources with regard to intelligence. In general, many local law enforcement agencies may not have an intelligence or analytic unit, reiterating what RAND found in 2004 when it reported that

> 64 percent of state law enforcement agencies reported having a separate criminal intelligence unit, as compared to only 10 percent of local law enforcement agencies.[102]

While many local police departments do not have an intelligence unit, they may have an analyst(s). However, even when local departments have an analyst(s) and were interested in detailing someone to the fusion center, they may not have enough man power to do so on a full time basis, and for many on a part time basis. There are many other cases where local law enforcement agencies appear unconvinced of the value of fusion centers — and by their cost/benefit analysis, it does not currently benefit the department to detail personnel to the center.

Non-Sworn Personnel from Law Enforcement Agencies. Although the majority of fusion center personnel come from law enforcement agencies, not all of them are sworn officers. It appears that most fusion centers have made a concerted effort to hire crime and/or intelligence analysts. In one case, a fusion center had tactically oriented, case support analysts, and more strategic analysts that managed specific threat portfolios, as well as non-sworn analyst supervisors.[103] Over the last two funding cycles, fusion centers have increasingly hired contract analysts using homeland security funds, although the length of the contracts has proved problematic for many fusion centers, which will be discussed further below.

---

[102] Lois M. Davis et al, *When Terrorism Hits Home: How Prepared Are State and Local Law Enforcement?*, available from [http://www.rand.org/pubs/monographs/2004/RAND_MG104.pdf] accessed on May 22, 2007, 44.

[103] Interview with Fusion Center Official, April 25, 2007.

Non-Law Enforcement Personnel. All-hazards centers are more likely than their counterterrorism or all-crimes colleagues to have non-criminal justice personnel,[104] to include Department of Health, Fire, Emergency Management Services (EMS), and other non-traditional homeland security partners in the public sector. Surprisingly, there were a number of fusion centers that had been described as all-hazards that did not have non-law enforcement personnel working in the center. In many cases, non-law enforcement public sector detailees to the fusion centers worked part-time and/or had a desk and were pre-cleared so they could work out of the center as needed and/or during an event.

Federal Participation. As will be addressed in greater detail below, almost all of the fusion centers studied for this report have some federal presence. The agencies represented, roles they play, and size of detailee staff differed significantly from center to center. To varying degrees, federal participation in state and regional fusion centers appears to influence the relationship between levels of government, state, and local access to information and resources, the flow of information/intelligence, and maturation with regards to intelligence cycle functions. Approximately 30% of fusion centers are collocated with a federal agency(s), and as a result, that federal agency(s) may have a significant influence on their development, operation, and even budget demands.

There appears to be a direct correlation between contact between a federal agency and a fusion center, and the center's positive outlook on the relationship between the two. In general, fusion centers collocated with a federal agency reported favorable relationships with that agency. This was often in stark contrast to the views of other fusion centers not collocated with a federal agency(s). For instance, one fusion center collocated with Immigration and Customs Enforcement (ICE) had nothing but praise for the agency, but another fusion center not collocated expressed frustration at not getting cooperation from ICE.[105] It should be noted that collocation and praise for inter-agency coordination does not necessarily translate to enhanced organizational effectiveness. Many fusion center leaders stated that collocation and the appearance of seamless coordination did not obviate the need to frequently inquire about information or an incident that was known to federal employees but not shared with state fusion center representatives.

Furthermore, fusion centers that were not collocated with a federal agency, but had a representative from a federal agency located full time in the center, were more likely to have a favorable impression of the relationship between the two than centers that lacked such a representative. Thus it is not surprising that many of the fusion center directors surveyed spoke of a close relationship with the local FBI entities: JTTF, Field Office, and FIG, given the large number of detailees from those entities.

---

[104] "Criminal justice personnel" is used to refer to personnel from both state, local, and tribal traditional police departments as well as corrections, parole, natural resource enforcement, alcohol enforcement bureaus, park police, etc.

[105] Interviews with state fusion center officials, April 12, April 17, and May 2, 2007.

Federalism and the Federal Role in Fusion Centers

One of the central, if implicit, themes that runs throughout this report is federalism. That is, while fusion centers were largely established by states, if the federal intent is to create a network of fusion centers that can be leveraged for both state, local, and federal public safety and homeland security purposes, there are several challenges that must be overcome. Research indicates one of the central challenges of designing a constructive and productive federal role in supporting these state and local fusion centers is working to ensure that the centers retain their state and local-level identity and support from those communities. According to many homeland security observers, one manifestation of this tension lies in the need to strike a balance between the national needs for a consistent provider of state and local threat information with the state's autonomy to pursue issues deemed of importance to local jurisdictions.[106] This tension is often notable when reviewing the diverse, and at times incompatible, types of threat and warning products required by state leaders and contrasted to those requested by federal homeland security and law enforcement entities.

Part of the challenge from the federal perspective has been how to guide, but not dictate to, the "owners and operators" of these largely state-established entities prior to the provision of any federal financial support. And, once federal financial and human resources support was provided, how to coordinate and target these resources for maximum overall return on investment.

Another example of how federalism flows throughout the fusion center issue is the legal treatment of terrorism. Terrorism is a federal crime. If it is prosecuted at all, it is usually done at the federal level. However, since the September 11th attacks, terrorism has been codified as a crime in many states.[107] Another example of how federalism permeates fusion centers is privacy. There is one Federal Privacy Act,[108] and numerous state privacy laws.[109] If fusion centers are serving both state, local, and federal ends, one of the central questions becomes what is the role of the federal government in supporting these centers, and what products and services can the federal government reasonably expect the centers to produce, given federal funding levels.

As elements of the states and regions they serve, fusion centers began to develop critical mass or staying power in the years immediately following the terrorist attacks

---

[106] With passage of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, DHS was given significant authorities for supporting state and local fusion center activities while undertaking efforts to improve information flow into the federal government for purposes of performing terrorism threat assessments.

[107] National Conference of State Legislatures, Summaries of Crime-Related Terrorism State Enactments, available from [http://www.ncsl.org/programs/cj/02terrorsum.htm], January 2003, accessed on June 19, 2007.

[108] See the Privacy Act of 1974, codified at 5 U.S.C, Section 552a.

[109] See National Conference of State Legislatures, available at [http://www.ncsl.org/programs/pubs/privacy-overview.htm] [accessed May 30, 2007].

of 2001. As these centers continued to proliferate across the country and garnered state support, federal entities began to take notice. While some 30 percent of the fusion centers interviewed were established prior to 2004, concrete federal financial support for the centers did not materialize until Fiscal Year 2004, when, according to DHS, it provided $29 million of Homeland Security Grant Program funding.[110] Federal guidance to the fusion centers followed shortly thereafter in July 2005. Finally, in 2006, human capital support in the form of DHS and FBI detailees to the centers began taking place.

While DHS has provided direct financial support to the fusion centers through the HSGP, the FBI has not provided direct financial support. The FBI's contributions have come more in the form of support for security clearances,[111] personnel support, and other "in-kind" contributions, such as rent payments when centers are collocated with FBI Joint Terrorism Task Forces or Field Intelligence Groups.[112]

The federal government has played several roles in assisting states and regions to develop their fusion centers, including the provision of:

- Recognition, post-9/11, of the need to have state and local governments and the private sector, non-traditional actors in national security matters, play an increasingly important role in homeland security.

- Guidance, to be adopted voluntarily by fusion centers, on the central elements of a fusion center and suggested methods for how to establish and operate sound fusion center policies and practices.

- Technical assistance and training related to issues encountered as fusion centers develop.

- Financial resources to support fusion center "start up" costs, including system connectivity.

- Human resources to assist in interaction with federal agencies and analytical fusion.

- Assistance to support enhanced information sharing between the federal government and state and local entities through the fusion centers.

- Congressional hearings on fusion centers.

---

[110] See DHS, Office of Grants and Training, *Fusion Centers: DHS Funded Activities — Fiscal Years 2004-2006*, April 2007.

[111] According to the FBI, it has obtained security clearances for 520 State and local law enforcement officers assigned to fusion centers. See FBI, "Fusion Centers," material provided to CRS from the FBI, dated May 25, 2007.

[112] See FBI, "Fusion Centers," material provided to CRS from the FBI, dated May 25, 2007.

- Promulgation of federal regulations.

Recognition of Homeland Security Role for Non-Traditional Actors

As alluded to above, the rise of state and regional fusion centers is part of a greater movement to decentralize homeland security to include non-traditional stakeholders (public health, emergency responders, and the private sector) at all levels of government (to include state, local, and tribal). The federal government appears to have recognized that the September 11th attacks signaled a need for greater state and local participation in homeland security. The 2002 *National Strategy for Homeland Security* acknowledges the expansion of responsibility for homeland defense and security, stating:

> The nature of American society and the structure of American governance make it impossible to achieve the goal of a secure homeland through federal executive branch action alone. The Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people.[113]

Even prior to the attacks of 9/11/2001, before the term "homeland security" was part of our national lexicon, the Department of Justice was working to ensure public safety and criminal information was shared across levels of governments. In 1998, the Department of Justice created the Global Justice Information Sharing Initiative (Global), a "group of groups" representing more than 30 independent organizations spanning the spectrum of law enforcement, judicial, correctional, and related bodies.[114] In October 2003, Global released *The National Criminal Intelligence Sharing Plan* (NCISP), which sought to:

> link federal, state, and local law enforcement agencies so that they can share intelligence information to prevent terrorism and crime.[115]

However, the NCISP does not explicitly address fusion centers and their role in information sharing fusion is not mentioned. It was not until July 2005 that federal fusion center guidelines were issued.

---

[113] U.S. Office of Homeland Security, The National Strategy for Homeland Security, July 2002, available from [http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf], accessed on May 22, 2007, p. 2.

[114] See U.S. Department of Justice, Office of Justice Program, Information Technology Initiatives, "Global Justice Information Sharing Initiative (Global)," available at [http://it.ojp.gov/topic.jsp?topic_id=8] (accessed June 1, 2007).

[115] U.S. Department of Justice, "Attorney General Ashcroft Announces Implementation of the National Criminal Intelligence Sharing Plan," Press Release, May 14, 2004, available from [http://www.usdoj.gov/opa/pr/2004/May/04_ag_328.htm], accessed on June 4, 2007.

Federal Fusion Center Guidelines

Under the aegis of the DOJ's Global,[116] Federal Fusion Center Guidelines have been developed, as recommended by the Homeland Security Advisory Council's Intelligence and Information Sharing Working Group in December 2004.[117] Global has issued two sets of Guidelines, and continues to work on additional guidance with, among other entities, the Office of the Director of National Intelligence's Program Manager for the Information Sharing Environment. The first set of Guidelines, entitled *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era — Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels — the Law Enforcement Intelligence Component* was published in July 2005.

The second set of Guidelines, entitled *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era — Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels — Law Enforcement Intelligence, Public Safety and the Private Sector* was published in August 2006. The federal Fusion Center Guidelines (FCG) received support from several law enforcement organizations, including the Law Enforcement Intelligence Unit (LEIU)[118] and Major Cities Chiefs Association (MCCA),[119] which added further credibility to the fusion center movement.

On balance, fusion center respondents had generally positive impressions of these voluntary guidelines. Fusion centers that were more advanced in their development when the FCG were released generally found that they validated their existing, policies, structures and activities. One center, however, found that the FCG were not helpful as the issues discussed were not tied to an over-arching national fusion center strategy and did not address technical aspects of operating a fusion center.[120]

---

[116] The Criminal Intelligence Coordination Council (CICC), an element of Global, recommended the establishment of a Fusion Center Focus Group which, in turn, was responsible for recommending guidelines for fusion center development. Fusion center representatives are included in Global, including the Vice Chair of the Global Advisory Committee, currently a colonel from the New York State Police. See [http://it.ojp.gov/topic.jsp?topic_id=8] (accessed June 1, 2007).

[117] See "Justice Department Releases Fusion Center Guidelines," in *Government Computer News*, August 31, 2005.

[118] Law Enforcement Intelligence Unit (LEIU), "Resolution in Support of Fusion Center Guidelines - Law Enforcement, Public Safety, and the Private Sector," Adopted on June 16, 2006, available from [http://it.ojp.gov/fusioncenterguidelines/leiuresolution.pdf], accessed on May 31, 2007.

[119] Major Cities Chiefs Association (MCCA), "Resolution: Fusion Center Guidelines," June 6, 2006, available from [http://it.ojp.gov/fusioncenterguidelines/chiefsresolution.pdf], accessed on May 31, 2007.

[120] Interview with regional fusion center official, May 3, 2007.

Fusion Process Technical Assistance Program

Consistent with many of the 18 Guidelines outlined in the aforementioned Fusion Center Guidelines, the DHS and DOJ-sponsored fusion process technical assistance program offers seven fusion center services in order to assist fusion center development. Instructors for these courses include fusion center and DHS representatives. The seven technical assistance services include (1) Fusion Process Orientation, (2) Fusion Center Governance Structure and Authority, (3) Fusion Center Concept of Operations (CONOPS) Development, (4) Fusion Center Privacy Policy Development,[121] (5) 28 CFR, part 23 (criminal intelligence systems), (6) Fusion Center Administration and Management, and (7) Fusion Center Liaison Officer Program Development.[122]

Research indicates that those fusion center representatives that have either participated in these services as trainers or students have found the sessions to have some utility. Others believe that, while the services were a useful first step, a more sustained form of fusion center mentorship, based on a national fusion center strategy, would add additional value to these brief courses.

Federal Financial Support for Fusion Centers

Federal financial support for fusion centers has largely come in the form of Homeland Security Grant Program (HSGP) funding. While the amount of funds recently provided by Congress to DHS to support state fusion center activities are unknown, past Departmental funding activities could be interpreted as somewhat confusing. The Consolidated Appropriations Act of 2008 provides DHS Office of Security and Office of Intelligence and Analysis funds to support state and local fusion centers.[123] In December 2006, DHS reported that it has "...provided over $380 million in support of these centers."[124] According to a DHS Office of Grants and Training (G&T) representative, this information includes the period from 2001 to the end of 2006.[125] Subsequently, in April 2007, DHS reported that in fiscal years 2004-2006, it provided a total of $131 million to "...establish or enhance a fusion center or

---

[121] According to the Deputy Program Manager for the ISE, a "Federal government-wide ISE Privacy Guidelines Committee has been established to ensure that incorporating the centers into the ISE will be done in a manner that protects the privacy, civil liberties, and other legal rights of individuals and corporations, as provided under U.S. law." See remarks of Susan B. Reingold, Deputy Program Manager, ISE, at the National Guard Bureau — J-2 Intelligence Knowledge Management Conference, June 12, 2007.

[122] See DHS Office of Grants and Training; Department of Justice, Bureau of Justice Assistance, *Fusion Process Technical Assistance Service*, January 2007.

[123] Funding numbers provided to DHS to support fusion center activities are not available as the figures are contained in the classified National Intelligence Program budget.

[124] See DHS Fact Sheet: *Selected Homeland Security Accomplishments for 2006*, December 29, 2006.

[125] Discussion with DHS, Office of Grants and Technology Official, June 6, 2007.

fusion cell."[126] If the $250 million "delta" between these two figures is attributable to time alone, that would mean that from March, 2003, when DHS was established, the Department allocated[127] approximately $250 million to fusion centers. While this is plausible, it may be unlikely, given the lack of DHS focus on fusion centers at that time[128] and the small number and relative immaturity of fusion centers in existence during the 2001-2003 time period. According to a DHS representative, the difference between the two figures lies in two factors: time and "requested" versus "actual" funding data.[129] Because data on actual funding lags data on requested funding, in order to provide the most up to date information, DHS G&T has used both figures. While this may be reasonable, even given DHS's methodological explanations, such wide variance in funding ($380 million versus $131 million) can be misleading.

Empirical research suggests that the figures cited by DHS as having been allocated to fusion centers do not necessarily reach the centers themselves.[130] This may represent a problem at the state level, as State Administrative Agents (SAAs) that administer HSGP funds may not always allocate funds in a manner that is entirely consistent with how the funds were requested. Alternatively, it could represent a problem with how DHS has defined fusion centers, and calculates the HSGP funding provided to the centers. One example offered by a fusion center leader noted that the center hired several analysts using HSGP funds but within a few months these personnel were reassigned to another non-fusion center homeland security effort.[131]

According to DHS, its methodology for calculating DHS-funded activities at fusion centers involves relying upon state and localities to report to the Department through use of the State Bi-Annual Strategy Implementation Reports (BSIR),[132] an

---

[126] See DHS, Office of Grants and Training, *Fusion Centers: DHS Funded Activities — Fiscal Years 2004-2006*, April 2007. The methodology section of this report stipulates that projects covered in the report included those that were "...reported directly to the (DHS, Office of Grants and Training) by State and local users of the Grants Reporting Tool (GRT), through the submission of their Bi-Annual Strategy Implementation Report." See cited report, p. 3.

[127] Allocation of funds differs from "draw down" of funds with the former referring to a DHS decision to support disbursement of HSGP funds related to fusion center to the State Administrative Agent (SAA) based on HSGP grant guidelines. "Draw down" is generally interpreted as the provision of the HSGP funds from the SAA to the fusion center or fusion center contractors for products and services provided.

[128] Interview with former senior DHS official, May, 2007.

[129] Ibid.

[130] Fusion center personnel are generally not the SAA for Federal grant funds and, as a result, may not necessarily know the explicit origins of HSGP Federal funds. However, respondent fusion center leaders or operational directors generally are aware of which information technology projects or human capital positions are funded with Federal HSGP grants.

[131] Interview with fusion center official, May 7, 2007.

[132] According to DHS officials, the BSIR reports require states to demonstrate "how the (continued...)

element of the Grants Reporting Tool (GRT).[133] DHS searches through the GRT databases using, among other methods, keyword search terms such as terrorism intelligence, emergency preparedness, response teams, fusion, analysis, and others. DHS recognizes this method has its limitations in terms of accuracy, as it has stated: "Because fusion center and/or fusion cell related projects may exist in the GRT that do not specifically use the term "fusion" in one of the search fields, this list of projects should not be considered to be all inclusive of DHS-funded fusion center activities nation-wide."[134] Moreover, the information on DHS-supported fusion center activities is based on grant recipients' entry of information into the GRT. While this method of calculation may serve DHS's purpose of articulating the specific projects funded related to fusion centers, there are a number of limitations associated with this methodology:

- Requested versus actual data could be stated more clearly. If both figures continue to be provided, historical percentages of requested amounts that are approved for actual funding might prove helpful.

- It speaks more to how HSGP funds may have been spent versus how they have been allocated. Notwithstanding the fact that Fusion Center Guidelines may not have been developed until 2005, if DHS and DOJ have been supporting fusion center "related" activities since 2001 when there were few fusion centers, the agencies should be able to ascertain the funding amount allocated to these activities.

- Grants allocated to fusion centers are done in a manner consistent with annual HSGP Guidelines which, while increasingly including direct language relating to fusion center activities, such as analysis of intelligence and information, are not specifically targeted to fusion centers. There is no "fusion center grant program." If it is a Departmental priority to develop a national network of fusion centers, it could be argued that a direct funding stream and/or HSGP Fusion Center Program might facilitate more targeted and tailored development of fusion centers. Alternatively, it could be argued that targeting fusion center funding more directly could undermine broader homeland security goals which transcend fusion center activities.

---

[132] (...continued)
actual expenditure of grant funds is linked to [the state's] strategy goals and objectives." J. Richard Berman, Statement before the Subcommittee on Emergency Preparedness, Science, and Technology of the House Committee on Homeland Security, April 12, 2005, available from: [http://www.dhs.gov/xoig/assets/testimony/OIG_1st_Responder_Testimony_Berman_Apr05.pdf], accessed on June 27, 2007.

[133] According to DHS officials, the Grants Reporting Tool was not available until 2004 and enhanced the Department's ability to track grants.

[134] See DHS, Office of Grants and Training, *Fusion Centers: DHS Funded Activities — Fiscal Years 2004-2006*, April 2007, p. 129.

In recent federal homeland security grant cycles, funds were permitted to be used to finance several fusion center-related activities and infrastructure investments. In a review of fusion centers nationwide, it appears that federal funding was likely to be used for start up costs and technology and infrastructure investment. In the last two years of homeland security funding, federal grants could be used to fund one- to two-year contractor slots for analysts at fusion centers. Additionally, federal grants were used to fund training for fusion center personnel. The salaries of federal employees detailed to fusion centers and the cost (rent, etc.) associated with collocation if a federal agency housed the fusion center, neither of which are funded through federal homeland security grants, are also represented in the overall federal contributions tallied in this report.

Another central question with respect to federal funding for fusion centers, not unlike other federal funding streams, is the extent to which it is reasonable to attach certain conditions to the funding. As mentioned above, one challenge is to retain the grass-roots, state and local priority basis of these centers. Yet, from a business perspective, it is not unreasonable for the federal government to expect some return for its investment in fusion centers. Other than generally enhanced information sharing, it is not certain what that return on investment is from the federal perspective. Part of this question may be resolved when decisions are made about the extent to which, if at all, the federal government determines sustainment funding will or will not be provided to the centers.

Sustainment Funding. One of the central questions and challenges to fusion centers continues to be the provision of sustainment funding, or funding which is provided annually, on a sustainable basis, to fusion centers to support personnel costs and information connectivity, among other functions. At the first annual national conference on fusion centers, Secretary Chertoff stated that one of the manners in which DHS has supported fusion centers is by providing grant funding — over $300 million — for the creation of fusion centers. However, he continued, the funding

> ... helps fledgling centers get off the ground and start to build fundamental baseline capabilities. This is not meant, by the way, to be sustainment funding. We are not signing up to fund fusion centers in perpetuity. But we do want to use these grants to target resources to help fusion centers make the capital investment and training investment to come to maturity. And then, of course, we expect every community to continue to invest in sustaining these very important law enforcement tools.[135]

At the same conference where Secretary Chertoff delivered his direct message that sustainment funding was unlikely, a representative of the Homeland Security Council (HSC) delivered a seemingly more sanguine message on this topic. According to the HSC representative, the Administration realizes that fusion centers are not a "fly by night operation," and, as a result, "... if we are asking you to invest

---

[135] Derived from CRS transcription of Secretary Chertoff's Keynote Address to the first annual National Fusion Center Conference, March 6, 2007.

resources...we need to remain committed."[136] The HSC representative stated that while there were no definitive percentage splits on burden-sharing, the Administration was having such conversations.[137]

Representative Jane Harman, having recently visited numerous fusion centers, raised concerns about fusion center sustainment funding, stating, "all the DHS staff assistants (detailees) in the world won't get the job done if fusion centers do not have adequate and sustained funding. Without money, they're going to disappear, and DHS State and local fusion center programs won't succeed.[138] DHS Chief Intelligence Officer, echoed Representative Harman's funding concerns,[139] testifying that

> I share many of the concerns expressed by this subcommittee ... about creating a sustainable fusion center capability at the non-Federal level. DHS, in partnership with DOJ, is a major supporter of fusion centers through our grants and accompanying technical assistance program, and in providing classified infrastructure....[140]

Alternatively, it could also be argued that if fusion centers can prove their tangible value to their state, local, and regional constituents support base, funding will continue to be provided through state and local revenue sources. Empirically, numerous respondent fusion centers shared that if federal funding is eliminated, it was likely that the center would continue to exist, but its activities would become far more parochial — by focusing largely on criminal intelligence relevant to the state and locality alone — and not issues pertaining to federal homeland security concerns.

What remains to be defined, and will be addressed below is, from a federal perspective, how is fusion center "maturity" defined, and how is it being assessed by the federal government, and according to what performance metrics? Given Secretary Chertoff's remarks, at what level of maturity do resources cease to be provided? Some argue that a federal fusion center strategy may be beneficial in addressing some of the historical fusion center concerns.

---

[136] Derived from CRS notes taken at the First Annual National Fusion Center Conference, March 8, 2007.

[137] Some conference participants noted that the seemingly contradictory messages were a demonstration of the lack of uniform federal policy with respect to State, local and regional fusion centers.

[138] See Transcript, House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Hearing on Security and Information Sharing and Civil Liberties, March 14, 2007.

[139] As part of the Intelligence Community, the budget of the DHS Office of Intelligence and Analysis (OIA) is classified. OIA's budget is combined with DHS' National Operations Center (NOC) budget and is classified under a general Departmental operations budget line.

[140] See Statement of Assistant Secretary Charles E. Allen Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the House Homeland Security Committee, March 14, 2007.

Human Capital Support

Research indicates that there are two levels of federal human capital support provided to fusion centers — individuals who have some level of contact with the centers as either local clients of the center and/or providers of information to the center, and part-time or full-time federal detailees to centers. The first category includes a relatively broad range of federal law enforcement and public safety professionals including representatives from the National Guard , Centers for Disease Control, High-Intensity Drug Trafficking Areas, as well as various DHS elements. The second category of part-time and full-time detailees to the fusion centers is composed largely, although not exclusively, of FBI and DHS representatives. While the FBI and DHS share certain missions, such as counterterrorism, they are unique agencies with distinctive missions and resource levels to meet their mission. Questions concerning the deployment of federal human capital resources to the centers might include

- To what extent have the FBI and DHS formally coordinated their deployments to fusion centers?[141]
- How did the FBI and DHS determine to which fusion centers they would deploy personnel?
- What criteria were used to support the decision?
- What types of professionals were deployed to the center?
- How have the FBI and DHS personnel currently deployed been utilized? What roles have they played and what value have they added to fusion center operations and analysis?

Table 1 below provides some data related to each of the aforementioned questions. What is notable is that it does not appear that the FBI and DHS drafted a joint, formal strategy outlining their approach to interaction with the centers. While each agency has its own unique mission, counterterrorism and countering crime are two large areas of mission overlap between these two federal agencies and the state and local fusion centers. Moreover, it also does not appear that the Homeland Security Council, a coordinating body akin to the National Security Council (NSC) primarily focused on homeland security issues, has issued a national strategy for fusion centers.

---

[141] According to the Deputy Program Manager for the ISE, the FBI and DHS are still developing an "integrated deployment plan." See remarks of Susan B. Reingold, Deputy Program Manager, ISE, at the National Guard Bureau — J-2 Intelligence Knowledge Management Conference, June 12, 2007. Given that the FBI has already deployed 250 personnel and DHS is in 15 centers, the effect such a plan may have at this point may be marginal. However, such a plan may prove useful if it clarified the roles and responsibilities of DHS and FBI detailees in the centers, and outlined a joint oversight process to monitor agency progress in effectively implementing those responsibilities.

Table 1. FBI and DHS Interaction with Fusion Centers

Issue	FBI	DHS	Coordination
Policy "engagement date" meaning date the agency began official interaction with fusion centers	Sept. 2005: FBI Dir. Mueller instructs all field leaders to "ensure coordination" between FBI and state-wide and multi-agency centers.	June 2006: Sec. Chertoff designates Office of Intelligence and Analysis as executive agent to accomplish the DHS state and local fusion center mission.	It does not appear that there was or is a national or FBI/DHS strategy for how the agencies planned to engage fusion centers to serve mission specific and/or overlapping counterterrorism goals.
Number of centers deployed to	35 of which, 16 fusion centers are collocated with an FBI entity	15	
Number employees assigned to centers	250	15, with a goal of 35 by the end of FY2008	
Types of employees assigned/deployed to centers	64 Special Agents; 121 Intelligence Analysts; 65 Other (linguists, investigative support specialists, financial analysts)	15 Intelligence Analysts/Intelligence Liaison Officers.	
Criteria for deployment	Center "maturity" (facility; connectivity; multi-agency full-time participation; "Global" guidelines biased)	Risk, maturity, field "needs assessments"	While both assessed maturity, it would appear DHS's assessment was largely risk-based.
Roles assigned/ deployed personnel play	Field Intel Group IA - analytical, information exchanges Special Agent - investigative links to Joint Terrorism Task Forces.	Information exchanges, "reach back" and liaison with DHS Headquarters for all DHS components.	Extent to which roles are coordinated and clear differ across fusion centers.

Sources: FBI material provided to CRS, May 25, 2007. DHS *Implementation Plan for State and Local Fusion Centers: Executive Summary*, June 2006.

While there are numerous issues that are raised by the lack of a comprehensive national strategy for what the federal government wishes to achieve through its interaction with fusion centers, one of the central issues becomes the allocation of

human resource to the centers. While risk,[142] maturity, and individual center needs[143] are entirely valid means by which to determine how to provide resources to centers, these funding criteria could result in numerous centers with significantly increased human resources, while others with arguably similar levels of risk remain in a stage of relative immaturity due to lack of human resource support. The question of what the federal government collectively defines as a "mature" center, or what the minimum level of capability for a fusion center is from a federal perspective, it could be argued, hampers the development of a long-term and sustained partnership between the federal government and the state and regional fusion centers.

"Lanes in the Road" — Roles and Responsibilities of Federal Detailees. Fusion center leadership often described FBI detailees as having well-defined roles and responsibilities compared to that of the DHS representatives whose roles in the organization were often less well-defined.[144] DHS officials claim to place Department representatives based on the needs and wants of the center. Thus, there appears to be a wider spectrum of roles for DHS personnel detailed to the various state fusion centers as their tasks vary from an intelligence analyst, to Departmental coordinators, to an advisor on federal grant applications. Yet all 15 DHS detailees come from the Office of Intelligence and Analysis. Some critics suggest that work undertaken outside of the core information sharing role between DHS and the fusion centers hampers the primary reason for being detailed to the center and negates any opportunity to "facilitate the flow of timely, actionable, all-hazard information between state and local governments and the national intelligence and law enforcement communities."[145]

---

[142] DHS calculated risk according to a quantitative and weighted model of the following 12 factors: population (10%), border risk (10%), terror risk (10%), immigration risk (10%), iconic value (5%), hazardous materials risk (10%), population density (5%), critical infrastructure (10%), port risk (10%), economic risk (10%), 2005 UASI funding (5%), 2005 State grant distribution (5%). See DHS, "The Department of Homeland Security Support Implementation Plan for State and Local Fusion Centers," March 7, 2006. According to DHS, "The key to harvesting the value from these relationships is in tailoring DHS' support offering to meet the specific needs of individual Fusion Centers." See DHS, *State & Local Fusion Center: DHS Support Plan*, February 2007.

[143] DHS has conducted over 17 site assessments, or visits to established centers to determine how it might best target human resources potentially provided to the centers. These visits include, but are not limited to, Columbus, Ohio; Phoenix, Arizona; North Central Texas; Albany, NW; Tallahassee Florida; and Maynard, Massachusetts. See DHS *State and Local Fusion Centers: DHS Support Plan*, February 2007. For a list of where DHS currently has personnel deployed see **Appendix B**.

[144] Conversations with Fusion Center Director, May 2007. Based on input from state fusion center leaders, DHS personnel detailed to a center performed functions ranging from analysis, DHS liaison and coordination point of contact, operations, providing grant writing expertise, logistics, and administrative.

[145] Statement of Charles Allen, Assistant Secretary of Intelligence and Analysis, Department of Homeland Security, before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, September 13, 2006.

Overall, relationships with DHS were described by fusion centers having a DHS detailee as relatively positive. However, by comparison, fusion centers reported a more favorable relationship with the FBI than DHS. There are numerous plausible explanations for such attitudes ranging from the different missions of FBI and DHS, to the sheer difference in numbers of FBI and DHS personnel assigned to these centers. Furthermore, it is likely that fusion centers, despite the traditional friction between state and local law enforcement and the FBI, are more comfortable with the FBI, because they share a common lexicon and world view that comes with being a member of the greater law enforcement community.

Corporate DHS is, however, a relatively new entity and in many ways state fusion center personnel — who are often sworn law enforcement officers — are still trying to determine how they interact with the Department. An example of this is the concern many state and local law enforcement and fusion center staff have expressed regarding sharing law enforcement sensitive information with the Department, which often has contractor analysts and other non-law enforcement personnel review data. On a few occasions, fusion centers mentioned steps they had taken to ensure DHS analysts would not be able to access various portals utilized by the center or participate in information sharing calls with other law enforcement agencies.

A common refrain from state fusion center leadership was that there was no coordination between the FBI and DHS with respect to substantive mission support and resource allocations were often duplicative or nonexistent. At present, the majority of terrorism-related issues that are brought to the attention of state fusion center entities are provided directly to the local JTTF, with the FBI[146] deciding to investigate the issue or returning the lead to the reporting agency.[147] However, DHS has also requested that all state fusion centers report any suspicious incident that may be perceived to be terrorist activity to the Department. Confusion exists whether this information should be transmitted to DHS' Office of Intelligence and Analysis, the DHS National Operation Center, or provided simultaneously to the DHS and the FBI JTTF. If the latter, homeland security observers are concerned that due to a lack of definitive federal roles and responsibilities crucial information may not be acted upon as DHS and the FBI will presume the other agency is undertaking the proper due diligence of ascertaining the viability of a potential threat.

The reporting chain problem — from state and local fusion centers to the Federal government — has been recognized. Under ISE Guideline 2, one recommendation is that DOJ and DHS, in consultation with the Program Manager's Office, develop standards to: (1) specify the means through which State, local and tribal data related to terrorist risks and threats and associated requirements and tasks is communicated to federal authorities and private sector entities and (2) develop, maintain and disseminate assessments of terrorist risks and threats gathered at the state, local or tribal levels, and (3) develop processes and protocols to ensure

---

[146] Presidential Decision Directive - 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, dated May 22, 1998, at [http://www.ojp.usdoj.gov/odp/docs/pdd62.htm].

[147] According to state fusion center leaders, it is quite common for a tip to be turned over to the JTTF without the center receiving additional information on its status.

Suspicious Incident Reports and Suspicious Activity Reports are reported to appropriate law enforcement authorities.[148] Implementation of this recommendation within fusion centers remains nascent and, therefore, inefficient dissemination procedures continue.

A related problem, that further highlights the lack of coordination between the federal agencies, is the vehicles for reporting and receiving information. As previously stated, fusion center officials expressed continued frustration about the multiple, seemingly competing, information systems promoted by various federal agencies. Entering the same data into multiple databases is time-consuming and inefficient. One fusion center official criticized DHS and FBI for failing to consider fusion center needs while promoting their own "favorite pet projects."[149]

Enhanced Information Sharing

In order to ensure that terrorism information[150] is shared "... among all appropriate federal, state, local and tribal entities, and the private sector through the use of policy guidelines and technologies...,"[151] Congress and the Administration created the Information Sharing Environment. Enhanced horizontal information sharing between federal agencies and vertical information sharing between all stakeholders across all levels of governments is the ISE goal. Located within the Office of the Director of National Intelligence, the Program Manger for ISE has been working to integrate fusion centers into a broad initiative to enhance information and intelligence between the federal government, and state and local law enforcement and public safety entities, as well as the private sector. The Homeland Security Advisory Committee believes that

> the concept of intelligence/information fusion has emerged as a fundamental process (or processes) to facilitate the sharing of homeland security-related information and intelligence at the national level, and, therefore has become a guiding principal in defining the ISE.[152]

---

[148] See ISE Guideline 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*, p. 21.

[149] Interview with a state fusion center official, May 3, 2007.

[150] Terrorism information is defined as "...all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threat posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." P.L. 108-458 §1016, codified at 6 U.S.C. 485.

[151] See the Intelligence Reform and Terrorism Prevention Act of 2004, §1016, P.L. 108-458.

[152] See U.S. Department of Homeland Security — Homeland Security Advisory Council, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and* (continued...)

According to its *Information Sharing Environment Implementation Plan* (November 2006), the ISE has or will take the following actions with respect to fusion centers:

- Establish a Federal Fusion Center Coordination Group "... to identify resources to support the development of a network of State-sponsored fusion centers charged to share information at all levels of the ISE, and will recommend funding options."[153]

- Encourage DHS and DOJ to "... work with Governors and other senior State and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the Federal government ..."[154]

- Encourage statewide and major area fusion centers to "ensure locally generated terrorism information is communicated to the Federal government through appropriate systems identified by Federal officials as part of ISE implementation."[155]

If, as mentioned above, one of the federal government's goals is to create a national network of fusion centers to share homeland security information in a timely and effective manner, these initiatives, once implemented will assist in integrating federal, state, and local public safety and law enforcement officials together. However, these initiatives do not necessarily, in and of themselves, constitute a national strategy for fusion centers, as they do not clearly articulate, among other factors, federal expectations of fusion centers, and the extent to which sustainment funding will be provided by the federal government for fusion centers.

With passage of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 11-53), the Interagency Threat Assessment Coordination Group (ITACG) was statutorily recognized as the federal agency responsible for facilitating the flow of finished intelligence products to state and local homeland security entities.[156] The participation of state and local personnel in the ITACG, located at the

---

[152] (...continued)
Information Fusion, April 28, 2005, p. 2.

[153] See Office of the Director of National Intelligence, PM-ISE, *Information Sharing Environment Implementation Plan*, November 2006, p. 119. According to a recent speech delivered by the Deputy Program Manager for the ISE, this center is established. The center, co-chaired by DHS and the FBI, "...is responsible for ensuring that the federal government's efforts to work with state and local fusion centers are coordinated and carried out in a manner consistent with the President's direction." See remarks of Susan B. Reingold, Deputy Program Manager, ISE, at the National Guard Bureau — J-2 Intelligence Knowledge Management Conference, June 12, 2007.

[154] Ibid.

[155] Ibid., p. 125.

[156] According to a conversation with a senior ODNI official in January, 2008, the ITACG (continued...)

National Counterterrorism Center (NCTC), allows state and local officials to develop an understanding of the volume and breadth of federal intelligence. Another objective of the ITACG is to allow federal Intelligence Community personnel to learn more about the types of information and intelligence that is valuable to state and local governments. Fusion center participation in the ITACG may be valuable, as the fusion centers represent a central point through which federal intelligence can flow across the country through appropriate dissemination channels and security procedures. At this stage of development, it is unclear what relationship the ITACG will have with state and regional fusion centers. A director for the HSAC stated that "DHS used to have its own way of sending out information, and the FBI did too...now [thanks to the ITACG] we have a coordinated way to send out threat assessment information."[157] However, there are some indications that the FBI and DHS will retain dissemination rights, thus calling into question whether the ITACG will streamline intelligence flow to state and local authorities, or exacerbate the current information sharing channel problems.[158] Some might suggest the ITACG would be the natural arbiter for fusion center information and intelligence coordination efforts.

Congressional Oversight and Funding

While fusion centers are not federal entities and, therefore, have no federal statutory basis, federal agencies with homeland security responsibilities appear to be relying heavily on the information gathered at the local level to support the development of a national threat assessment. Congress plays a role in supporting these centers and federal government homeland security efforts in at least two areas. First, as mentioned above, it authorizes and appropriates both HSGP funding, some of which is allocated to support fusion center related activities, and the National Foreign Intelligence Program (NFIP) budget which supports DHS and FBI personnel detailed to the centers. Second, Congress has held numerous hearings to learn more about fusion centers. Notably, during the 109th Congress there were over five hearings held related to intelligence sharing, DHS Intelligence, and fusion centers. Federal witnesses included representatives from the FBI, DHS, and Office of the DNI. There were also numerous witnesses from state and local agencies, including, but not limited to, the Illinois State Police, the Virginia Fusion Center, the New Jersey Office of Homeland Security and Preparedness, and the Commonwealth of

---

[156] (...continued)
has accomplished the following: (1) a DHS official is currently the Director of the ITACG with an FBI serving as the Deputy Director, (2) the NCTC has allocated space for the agency, and (3) two state and local officials have been detailed to the ITACG with two other detailess to join the office in the coming months.

[157] Quoting Thomas Bossert, Jason Miller, "White House Council Puts Cybersecurity in Focus," FCW.com, July 2, 2007. [http://www.fcw.com/article103121-07-02-07-Web].

[158] According to a conversation with a senior ODNI official in January, 2008, the ITACG is incurring significant challenges while attempting to meet the statutory mandates of the agency. Reportedly, the ITACG has had difficulty in having senior officials of the NCTC, DHS, and FBI agree on the role and responsibilities of the organization. It was also noted that the NCTC has developed an organization that is coordinating with, and providing intelligence products to, state and local homeland security entities.

Massachusetts. Thus far in the 110th Congress, there have been at least five hearings related to state and local fusion centers, with one hearing taking place in Washington State. Witnesses have included representatives from the private sector, including The Boeing Company and Pacific Northwest National Laboratory, and individuals from state and local fusion centers in Florida, Tennessee, and Delaware.

DHS-OIA funding levels are classified as a result of OIA being a member of the U.S. Intelligence Community.[159] As a result, the level of DHS-OIA budgets allocated to detailing intelligence professionals to fusion centers is unknown. In another indicator of congressional interest in increasing funding to the centers, P.L. 110-28, the "U.S. Troop Readiness, Veterans Care, Katrina Recovery, and Iraq Accountability Appropriations Act of 2007," provided an additional $8 million to the DHS Analysis and Operations account "... to be used for support of the State and Local Fusion Center Program...."[160]

Promulgation of Federal Regulations — 28 CFR, Part 23

As mentioned above, all fusion centers are guided by federal regulation 28 CFR, Part 23 with respect to how they manage their multi-jurisdictional intelligence systems operating under Title I of the Omnibus Crime Control and Safe Street Act of 1968 (P.L. 90-351). 28 CFR, Part 23, requires all multi-jurisdictional law enforcement information management systems funded in part by federal grants[161] to follow guidelines for the collection, storage, and purge of information. 28 CFR, Part 23 states that information stored in such a system must be "reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years."[162] It is based on a "need to know" and "right to know," which are not explicitly defined terms. Rather, 28 CFR, Part 23, calls upon each project to establish their own written definitions.[163]

---

[159] See P.L. 107-296, Section 201(h), codified at 50 U.S.C. 401a.

[160] See P.L. 110-28, Title I, Chapter 5. The language requires quarterly reporting to the House and Senate Appropriations Committees on numerous factors relating to fusion centers.

[161] Not all federal grant streams potentially used for funding such systems are included in 28 CFR, Part 23 - currently any systems funded in part by "all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program sub-grants,"DOJ, *28 CFR Part 23: Criminal Intelligence Systems Operation Procedures*, available from [http://www.it.ojp.gov/documents/28CFR_Part_23.PDF], accessed on June 1, 2007, known hereon as DOJ, *28 CFR Part 23*, - This includes "any Office of Justice Programs (OJP) and Bureau of Justice Assistance (BJA) programs, such as the Byrne Formula or Discretionary Grants Programs, the Local Law Enforcement Block Grant (LLEBG) Program, and Community Oriented Policing Services (COPS) grants", while others like HIDTA programs and apparently Homeland Security grant funds have adopted it as policy, although it is not in statute.

[162] DOJ, *28 CFR, Part 23*, 4.

[163] Ibid., p. 3.

In many ways, 28 CFR, Part 23, may be outdated and in need of evaluation against the backdrop of the current threat environment. 28 CFR, Part 23, is focused on traditional crime, not terrorism. As such, it has relatively short information retention periods which may not necessarily be consistent with known terrorist planning cycles and/or the need for historical data for terrorism threat assessment.[164] Furthermore, this federal regulation was written before many of the data storage and data-mining technologies were available. It is unclear whether some of the technological devices available today, like those that allow users to query disparate databases which are not directly connected, would fall under the jurisdiction of 28 CFR, Part 23. The regulations also promote a "need and right to know" standard, which has been judged as one of the factors contributing to the (real or perceived) "wall" between intelligence and law enforcement at the federal level that prevents effective information flow. Finally, it could be argued that 28 CFR, Part 23, is too vague in parts because it allows agencies to define their own terms, like "need to know," which could contribute to vastly different standards across jurisdictions and, ultimately, ineffective information sharing.

Private Sector Purposes and Roles in Fusion Centers

The relationship and role of the private sector is a function that most state fusion centers have yet to fully define and/or embrace. A number of the fusion centers surveyed have undertaken informational and security-related discussions with some of the major critical infrastructure owners and operators and data-providers within their respective jurisdictions. However, while acknowledging that a comprehensive understanding of the risks to the state/region is impossible to attain without a viable relationship and consistent information flow between the center and the private sector entities within the center's jurisdiction, the vast majority of centers have yet to put the processes in place to support such an endeavor. Very few of the state and regional fusion centers have an infrastructure sector representative detailed to their organization and rely, in part, on open-source information, data provided by the federal government, or contract data vendors for information about threats to a critical infrastructure facility. Common reasons for the lack of a relationship between the fusion center and private sector entities are

- prioritizing the infrastructure sectors to be represented in the center based on risk;
- a lack of appreciation as to the role and information a sector representative might provide; and
- the lack of a federal government strategy or recommendations regarding how the fusion center should incorporate private sector data into the analytic fusion process.

---

[164] Angel Rabasa et al., Beyond Al Qaeda: Part 1 — The Global Jihadist Movement, (RAND, Santa Monica, CA, 2006), available from [http://www.rand.org/pubs/monographs/2006/RAND_MG429.pdf], accessed on June 13, 2007, 63-71.

Information Sharing and Analysis Centers (ISACs)

Although representative ISAC organizations have different mandates and provide different types of information and services, generally the entities provide its members data related to threats, vulnerabilities, pending legislation, and issues of concern to a specific infrastructure sector. ISAC organizations, originally envisioned as a mechanism for the sharing of critical infrastructure information between partnering corporations and with the federal government[165] currently are not being fully utilized by state and regional fusion centers as a resource for information. One option for fusion centers is to enhance their relationship with private sector organizations through the establishment of education and information-exchange efforts with ISAC representative organizations. Some homeland security observers suggest that the building of a productive relationship with private sector entities may allow the fusion center to enhance information sharing efforts with operators of the state's critical infrastructure and assist in the preparation and prevention phase of homeland security.

Protected Critical Infrastructure Information (PCII)

The Protected Critical Infrastructure Information (PCII) Program[166] may also be a venue that would allow a fusion center to be in the best possible position to effectively assess risks within its jurisdiction and/or respond to a potential situation at a critical infrastructure facility. If DHS is authorized by the private sectors engaged in this effort to disseminate this information to state and regional fusion centers, it may allow state and local officials to approach potential situations of concern with knowledge of hazardous critical infrastructure vulnerabilities that may place the state/region at greater risk. Should PCII data be authorized for sharing with state fusion centers, the information may enhance state and local authorities plans for incident response coordination efforts.

---

[165] The goal of Presidential Decision Directive (PDD) - 63 was to assure the security of the United States' vulnerable and interconnected critical infrastructures. With the signing of Presidential Decision Directive - 63 in May, 1998, the private sector was encouraged to establish numerous ISACs for the purpose of having a representative entity from which the sharing of critical infrastructure information threat and vulnerability data would occur between the federal government and the owners and operators of the nation's life-sustaining utilities. In December, 2003, PDD-63 was superseded by Homeland Security Presidential Direct - 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, however the federal government's requirement to "continue the encouragement and development of information sharing and analysis mechanisms" still exists.

[166] The DHS's Protected Critical Infrastructure Information (PCII) Program is designed to encourage private industry to share its sensitive security-related business information with the federal government. DHS and other federal, state, and local analysts use PCII in pursuit of a more secure homeland, focusing primarily on: analyzing and securing critical infrastructure and protected systems, identifying vulnerabilities and developing risk assessments, and enhancing recovery preparedness measures. See [http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm].

Privacy Concerns and Private Sector Data Use by the Federal Government

As stated throughout this report some homeland security observers note that increasing the universe of available information does not necessarily translate into a better understanding of the risks to a geographic location or infrastructure sector. Since 9/11, many programs have been established or enhanced for the purposes of searching for signs of terrorist activity in a central repository to assist with information collection, trend analysis, and spotting of anomalies.[167] Of note, the DHS Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) program, which is being developed to "analyze large amounts of data, such as the relationships among people, organizations, and events"[168] when fully functioning may have the ability to receive and provide information to the nation's fusion centers to assist with analytic strategic indications and warnings. Should ADVISE or other data collection and analysis programs become fully functional and accessible by fusion centers, some might see this as a devolution of national intelligence capabilities from the federal government to state governments resulting in the encroachment on individual civil liberties. Some are concerned that as fusion centers and the IC agencies codify relationships, there is increased potential for misuse of private sector data. It could be argued that such a relationship will allow state entities to act as agents of the federal government in performing federal intelligence community activities that violate federal privacy laws.

Fusion Center Challenges and Potential Options for Congress

Given that fusion centers are entities established by states, localities and regions to serve their own criminal, emergency response, and terrorism prevention needs, and the sensitivities associated with federalism, there may not necessarily be a federal remedy to every fusion center-related issue identified in this report. Moreover, there is a direct correlation between federal remedies to issues affecting fusion center development, and the extent to which Congress wishes to condition the funds it authorizes and appropriates for such centers. As a result, there are at least two categories of challenges and potential options: (I) those challenges for which there are unique federal remedies and (II) those challenges for which there are no unique federal remedies, and may be more oriented toward possible state or level governmental intervention. Congressional remedies could potentially involve a broad range of possible actions including, but not limited to, oversight of federal agencies and entities engaged in interaction with fusion centers, requesting Executive Branch action on any number of fusion center-related issues, establishing a statutory basis for fusion centers, convening additional hearings which include state and local fusion center leaders as expert witnesses, adjusting future funding levels for fusion

---

[167] See CRS Report RL31798, *Data Mining and Homeland Security: An Overview*, by Jeffrey Seifert.

[168] Government Accountability Office, *Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs are Developed,* March, 2007, p. 11.

centers, and/or considering the extent to which, if at all, any future federal funding may be conditioned on certain performance benchmarks being met.

I. Federal Challenges and Potential Options for Congress

Given the stated need to develop a national network of fusion centers, and that a certain amount of financial and human resources have been devoted to assisting the states and regions develop their fusion centers, the following represent challenges and options that the federal government and, specifically, Congress may wish to consider.

Option 1: Draft a National Fusion Center Strategy

Notwithstanding the fact that individual federal agencies and offices may have their own strategies concerning their interaction with state and regional fusion centers, there remains *no definitive national strategy on fusion centers*. One option for Congress is to recommend the executive branch draft a cross-agency national strategy with input from the FBI, DHS, ODNI - PM-ISE, DOD and other Intelligence Community, and state and regional fusion center representatives. Should such a strategy be determined desirable, it might address the following issues:

- **Ownership and benefits.** Who "owns" fusion centers and who benefits from their work?
- **Federal versus SLT roles and responsibilities, to include funding.** What is an equitable division of labor and costs?

- **Permanence — statutory basis and sustainment funding.** If fusion centers play an important homeland security role, should they be provided a statutory basis at the federal level? If continued federal funding is being contemplated, how might it be structured to yield the most productive outcome for federal, state and local fusion center clients?

- **Ultimate goals and performance measures.** What gaps do fusion centers fill and how does the federal government measure performance?

- **Coordinated federal interaction with fusion centers.** How does the federal government ensure the various agencies engaged in homeland security have a coordinated plan for fusion and efficient interaction with fusion centers?

- **Relationship between fusion centers and the Federal Intelligence Center.** How closely, if at all, should fusion centers be integrated into the federal intelligence community? Are fusion centers members of the intelligence community, adjuncts or partners with the intelligence community, a proxy information source, or an unrelated and parallel information effort?

Pros and Cons. There are many arguments in favor of the creation of a national strategy for fusion centers. Such a strategy would likely create coherence to what could be argued is currently a somewhat ad hoc and informal approach to fusion centers. Some might argue that without such a overarching national strategy, fusion centers will only provide limited benefits to limited consumers. Arguments against this option might include disruption to ongoing activities, or that such a strategy, while not formal, already exists in the form of the collective activities of DHS, the FBI, Global Justice, and the Office of the Director of National Intelligence's Program Manager for the ISE. Furthermore, to be successful in creating a cohesive structure for forty+ fusion centers across the country, a national strategy may need to deal with several politically sensitive issues, such as the need for a joint deployment strategy for the federal agencies that detail personnel to state and regional fusion centers. However, if this issue and other sensitive topics are not comprehensively addressed and resolved, fusion centers may have limited national impact. The strategy's potential for success is likely to hinge on the perception of input by all-levels of government and sectors, and the means used to implement the goals and objectives outlined in the strategy.

Option 2: Answer the Sustainment Funding Question

While respondent fusion center leaders had many high priority items concerning their interaction with the federal government, the question of sustainment funding was foremost in their minds. Should federal funding to fusion efforts be continued? To what end? And how conditional does Congress want federal aid to fusion centers to be? The current regime of HSGP funding includes some limited conditions for funding fusion centers. However, the Fusion Center Guidelines remain entirely voluntary even for recipients of federal HSGP funds. As a result, for example, the federal government has no formal and systematic means of auditing whether each center is appropriately protecting civil liberties, or using federally funded intelligence analysts in a manner that is consistent with national goals and objectives for fusion centers, should they be explicitly defined. As outlined above, should Congress determine it wishes to take action on this option, a range of possible legislative tools are available, as discussed below.

2a. Status Quo. The most obvious option is to continue the current manner of funding — that is, using the HSGP grants as the federal mechanism to make funding available for states and localities for potential allocation to state and regional fusion centers. This process is reliant on state grant applications, and the flow of federal funds to state/regional fusion centers is largely determined by the sub-federal designees that make homeland security grant allocation decisions within each state and/or municipality. Furthermore, fusion centers compete with a wide range of homeland security initiatives for funding. While certain elements of HSGP funding are geared toward supporting fusion center development, there is no targeted funding stream directly allocated to fusion centers themselves.

If the approach to funding fusion centers remains the status quo, then Secretary Chertoff's statement that DHS has not "... signed on to fund fusion centers in perpetuity...." will remain true. Without a dedicated funding stream, and/or another large-scale terrorist attack within the United States, it is unclear whether fusion

centers will continue to receive federal funding, as well as sub-federal resources, to continue their current functions as outlined in this report.

Pros and Cons. Arguments in favor of maintaining the status quo include those who suggest such an option would result in a natural progression of the current funding model. It would allow for a certain amount of continuity in funding streams and methods of allocating funds. Such an option would likely result in minimal HSGP program disruption. Arguments against this option might include that the status quo would continue to leave the fundamental sustainability question — one that is foremost in the collective mind of fusion centers — unanswered. Maintaining the status quo may have a drawback as it might perpetuate uncertainty about sustainable federal aid. This uncertainty might continue to hamper how fusion centers plan their information technology and human resource needs for the future.

2b. Status Quo "Plus" — Enhance Flexibility of the Current HSGP or Establish a Fusion Center Grant Program Within HSGP. Under this potential option, the current grant program could be slightly altered to address some of the oft cited hurdles that state and local officials believe impede the flow of federal grant funds to fusion center projects. Two such alterations to be considered include

- Increasing the duration of grant cycles in order to allow for enhanced continuity and human resource planning, particularly for contract-supported intelligence analysts.

- Building some level of autonomy into the HSGP "80/20" localities/state split of HSGP funding to allow state political leadership some autonomy to re-allocate a portion of overall HSGP funds to a single, designated state-wide fusion center. Such flexibility could be conditioned on formal HSGP audits to ensure accountability and that funds re-allocated within state HSGP awards are consistent with the state's fusion center mission and Federal Fusion Center Guidelines. These audits would include input from fusion center leaders, State Administrative Agents, and the state's Homeland Security Advisor.

A more significant adjustment to the existing HSGP that could potentially alleviate some of the difficulty associated with facilitating the flow of federal homeland security funds to fusion centers is the creation of a narrowly targeted "Fusion Center" grant category, similar to the Port Security Grant Program (PSGP) and the other four sub-categories included under the Infrastructure Protection Program (IPP).[169] If such a program were established and funded, arguably, it could provide the federal government with increasing leverage to condition the funding on a number of factors, not the least of which may be compliance with Fusion Center Guidelines, or other, more specific fusion center performance metrics.

---

[169] Homeland Security Grant Programs - FY2007 Information available from [http://www.ojp.usdoj.gov/odp/grants_programs.htm#fy2007ipp], accessed on June 14, 2007.

Pros and Cons. Arguments against this option might include the position that such a program might set a precedent for other more narrowly tailored homeland security oriented programs to advocate for a similar approach. It could also be argued that such a program might undermine the current federal approach to fund the functions which underlie homeland security — such as information sharing and analysis. Alternatively, it could also be argued that there are several existing programs that are narrowly tailored to ensure that risks and capabilities determined by the federal government to be nationally critical are already funded in this manner (such as the Buffer Zone Protection Program (BZPP), and other Infrastructure Protection Program (IPP) grants). If the federal government determined that state and regional fusion centers provide a critical homeland security function, both protecting critical national infrastructure and transportation security, might it not be prudent to have a fusion center grant program?

2c. Develop a Sustainment Funding Approach. If it is determined that establishing a national network of fusion centers serves long-term, national homeland security interests, it may be reasonable to design a system which provides resources to state and local fusion centers commensurate with the national benefit derived. This presupposes the development of (1) a cogent set of concrete national interests served by fusion centers, (2) a set of metrics that can quantitatively capture how well fusion centers are meeting these interests and goals, (3) standards for "minimum levels of capability" and fusion center "maturity,"and (4) thresholds linking levels of maturity to levels of federal funding. These standards and metrics could be developed as part of a cooperative endeavor between federal, state, and local representatives, possibly under the "Global" program. As with other options above, the extent to which Congress could condition such an approach is an open question.

Pros and Cons. One of the primary arguments that could be made against this option is that it is too complex and, as a result, would be difficult to implement and may encourage states to "game the system" so as to remain immature enough to retain federal funding. Alternatively, arguments in favor could be that Congress is responding to fusion center requests for a long-term and explicit federal approach to sustainable funding. While the states may not like the performance metrics developed and/or the thresholds for funding phase-outs, these metrics and standards would at least create an environment of certainty in which states could better plan and target state and local funding streams to meet their ongoing funding needs that the federal government has clearly informed them it will not meet. If this option is pursued, metrics development and center evaluation would likely be most effective if designed and undertaken with fusion centers and SLT agency sponsors to ensure they are not resisted or rejected.

2d. Direct and Sustainable Fusion Center Functional Support. Alternatively, Congress alone, or with input from DHS, the FBI, and the ODNI's PM- ISE, could determine that there are certain fusion center functions that provide direct value and benefits to the federal government, and as such, warrant sustainable federal financial support. For example, it might be determined the development of state-wide intelligence systems, and information and intelligence analysis, are two core fusion center functions that are clearly linked to the federal benefit derived from fusion centers. As such, the federal government could determine that it would support these functions directly and possibly in a sustainable manner. If such a

decision were made, a pilot program might be established and implemented at certain fusion centers over a specified time period to ascertain empirical federal benefits derived from direct support of such functions.

Pros and Cons. Arguments against this option might include that such an approach goes beyond what some in the federal government have stated the government will support, and could increase federal outlays beyond levels currently being supported, and might create a sense of entitlement among fusion centers. Arguments in favor of this option are that such an approach would provide fusion centers with a sense of certainty about federal funding. If, for example, fusion centers knew Congress would support funding for intelligence analysts, they would no longer need to budget for such personnel. It could also be argued that such an approach would be relatively simple — after a period in which seed funding is provided and centers reach maturity (as judged by the federal government), centers would get some level of sustainment funding for a relatively specific function or set of functions subject to a pilot program's assessment of output that benefits national interests. Some lessons could be learned from the federal government's other grant program experiences, including the Community Oriented Policing Program model.[170] It could be argued that federal support and cultivation of the relevant skills and capabilities within fusion centers that provide direct benefit to the federal government may result in state and regional fusion centers acting as a "force multiplier" for federal efforts.

Option 3: Training

Given that effective information/intelligence fusion and proactive approaches to all-hazard prevention and preparedness depends on a common understanding of intelligence and information and the potential uses thereof, an argument can be made for enhanced and uniform fusion center training. Research indicates that the diversity of types of professionals serving in fusion centers can lead to differing perspectives, or possibly, competing visions for the fusion center. Retired military intelligence officers may approach intelligence differently from, for example, state first responder personnel. While neither approach may be "best" and the center might benefit from diversity of opinions, a common understanding of and lexicon for intelligence and its benefits and limits amongst all level of fusion center personnel can go a long way toward ensuring cohesiveness, clarity of vision, and productivity of a fusion center.

In addition to intelligence training, some homeland security observers note that fusion centers may benefit from additional and standardized civil liberties training. Most fusion centers surveyed claim to have institution-wide civil liberty training and awareness activities that ensure all employees are aware of how personal and corporate information can be collected, received, stored, and combined with traditional intelligence community information toward producing a risk assessment

---

[170] Analogies to other Federal programs do, however, have limitations, as any pilot program would have to assess the potentially unique national interests served by fusion centers. For example, while hiring local police to prevent crime may serve the national interest, does the prevention of terrorist attacks (another crime) serve the national interest more or less than general violent crime prevention at the State and local levels?

for a given issue of concern. However, this training is often agency-specific and there may be differences between state activities and federal expectations. As such, the federal government may wish to require a part of all funding allocated toward a state fusion center be used for nationally consistent civil liberties training with special attention to concerns surrounding the use of private sector data. Another option would make such training a precondition for receiving federal grants. Should Congress wish to pursue this option, a range of possible legislative tools are available, including designating a federal government entity (See Option 4f) to provide oversight of these efforts, amongst others, as discussed below.

3a. Philosophy — Develop National Intelligence and Information Lexicon and Standards for Fusion Centers. Congress may consider requiring the Intelligence Community to work with law enforcement (State, Local, and Tribal (SLT) and federal) to develop a common lexicon and definitions for intelligence, information, situational awareness, and other key concepts to ensure all entities, at all levels of government, that are engaged in homeland security are working from the same play book. These basic definitions and standards may be applicable whether the information/intelligence is national security-related or criminal in nature. The PM - ISE, which is currently working to reconcile different sensitive but unclassified security designations and handling instructions, might be a natural coordinator for such an effort. The creation of enhanced and standardized, national fusion center training could help promote this common "dictionary of intelligence."

Pros and Cons. Arguments in favor of this option might include that the lack of clarity between a "pure" intelligence and criminal intelligence role leads to over-aggressive or under-aggressive intelligence postures in fusion centers. In short, clarity would lead to greatly enhanced information sharing. Arguments against this option could include a fundamental disagreement with the belief that there is a difference between "pure" intelligence and criminal intelligence — both seek to prevent man-made threats, including crime and terrorism. Therefore, no additional training is needed — fusion centers understand the legal regimes under which they operate. Another argument against creating these standards and common definitions is that it is likely to be a difficult undertaking given the sheer number of agencies involved and remnants of ownership culture that still persist within the federal Intelligence Community.

3b. Enhance Civil Liberties and Privacy Training. Given the potential for privacy and civil liberties violations to substantially undermine the public support for fusion centers, enhanced and periodic re-fresher training in civil liberties may be a valuable tool for fusion center personnel. While all respondent fusion centers were cognizant of the need to protect civil liberties and provided initial training on privacy and civil liberties protection, in general, this was one time, static training. Enhanced training might include in-state or national instances in which violations of privacy and/or civil liberties occurred and possible lessons learned from those instances. Moreover, annual re-fresher training that emphasizes how First Amendment protected activities differ from speech which incites violence or sedition, may be useful. In addition, the adoption of national standards and/or guidelines in this area would support this effort. There have been some efforts in this area - PM-ISE issued privacy guidelines for the information sharing environment in December 2006, which

are available to the public and could be utilized by fusion centers.[171] It could be argued, however, that these guidelines aren't likely to have a significant impact on state and regional fusion centers in their current form, as they are too vague, only focused on federal agencies, and entirely voluntary.

Pros and Cons. Arguments against this option may be resource-based — that is, training resources may not allow for such training. Arguments in favor of this option may include an understanding of history. The lessons of COINTELPRO, the period of domestic intelligence abuses in the late 1960s and early 1970s, necessitate such training. It may also be worth examining the training related to 28 CFR, Part 23, which was adopted in response to COINTELPRO abuses.

3b-Part II. Enhance Training of 28 CFR, Part 23. With regard to training on 28 CFR, Part 23, the federal regulation governing multi-jurisdictional intelligence systems, many law enforcement agencies involved in fusion centers (often because the latter were an outgrowth of the former) reported that they had received some training from DOJ and/or other contractors on the regulation when they first began operating an intelligence management system. In many cases, that training took place many years ago and the agencies in question have had little to no follow up training. Many didn't know who at DOJ to contact in the event that the fusion center had a 28 CFR Part 23-related question or what office fielded additional training requests. Almost all fusion centers interviewed for this report facilitated 28 CFR Part 23 training for their staff either through the center directly or via the state police or bureau of investigation. As this is taking place at the state and local level, it is unclear if there is a consistent application of 28 CFR. Currently, fusion centers are in the difficult position of being urged to be proactive to help prevent future attacks, while simultaneously being warned about being too aggressive.

Additional and periodic training to fusion centers might be considered, even if their parent state police/bureau of investigation agency and other law enforcement participants have already received such training at some point in their development. Consideration may also be given to providing legal resources for fusion centers that want an external legal opinion on their collection, storage, and dissemination activities.

Pros and Cons. Some might argue that the advantage to this type of additional and periodic training is that it might help eliminate questionable intelligence practices, clarify legitimate activity, and ensure the protection of civil liberties. The availability of additional legal resources to fusion centers and SLT law enforcement agencies may result in better and consistent legal advice and assist resource-strapped entities that are currently suffering a fiscal crisis. Arguments against such training might be resource-based. Furthermore, if 28 CFR is going to be revised (Option 6a,

---

[171] PM-ISE, Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of Information Sharing Environment, December 2006, available from [http://www.ise.gov/docs/ise%20privacy%20guidelines%2012-4-06.pdf], accessed on June 27, 2006.

page 69), training on what could be viewed by some as the "old regime" may not seem productive.

3c. Establish a Fusion Center Mentor Program. As mentioned above, when fusion centers have had an opportunity to avail themselves of the DHS/DOJ Technical Assistance Program attest, the program seems quite beneficial. However, the support is provided over the course of a few days and many fusion center respondents desire longer-term and sustainable assistance, the type characteristic of traditional mentoring programs. While some fusion centers have created informal mentoring programs of their own, a more formal program could be designed that would flexibly pair centers of varying levels of maturity with one another to share best practices and means of surmounting what may be common obstacles to fusion center development.

Pros and Cons. Arguments against this option may be that it is essentially superfluous as informal mentor relationships are already being established by the proactive outreach of fusion center leaders either informally within their region, or at fusion center conferences. Moreover, fusion center conferences and the DHS "Lesson Learned" website[172] provide an opportunity for centers to conduct liaison and share best practices formally and informally. Arguments in favor of this option include the position that such a program would constitute a relatively minor addition to the Technical Assistance Program in terms of resources. The program could facilitate the pairing up fusion centers they believe could learn from one another. While official guidelines for the mentor relationships may not be necessary, the federal government might require any new lessons learned be added to the DHS Lessons Learned Information Sharing database.

3d. Enhance Private Sector Outreach and Information. Some homeland security observers view the relationship between state fusion centers and the private sector as one of both unlimited potential and great concern. Currently, most fusion centers describe an interest in expanding their relationship with the private sector in their jurisdiction, but consistently, most fusion centers were admittedly behind in developing those relationships. Information sharing with the private sector was often ad hoc and inconsistent. Furthermore, it is important to note that fusion centers did not appear to be systematically importing and incorporating private sector data into their information/intelligence fusion efforts, although some expressed an interest in better utilizing private sector data in some form.

It is important, however, to identify the opportunity to introduce new types of data, including those from private sector sources, into the intelligence fusion process to allow for a comprehensive risk assessment to a given geographic environment or infrastructure facility. It may be that the data pointing to a pending attack cannot be understood in context unless all knowable information is available for assessing. On the other hand, absent strenuous civil liberty protections and safeguards the possibility for misuse of personal or corporate data looms over many fusion center

---

[172] Form more information on the Lessons Learned Information Sharing (LLIS) website visit [http://www.ojp.usdoj.gov/odp/docs/LLIS_FactSheet.pdf] and [http://www.llis.gov], both accessed on June 14, 2007.

activities the state may undertake in partnership with or support of private sector organizations. Furthermore, it could be argued that massive private data collection and analysis efforts are wasteful and a better use of resources would be to follow known criminal leads rather than sifting through an enormous amount of data looking for possible signs of terrorism.

Pros and Cons. Arguments in favor of increasing interaction between fusion centers and the private sector focus mostly on increasing the availability of possible terrorism-related information. Should the federal government and private sector routinely share information some believe this will lead to a better understanding of the threat environment which in turn may deter or defeat future terrorists attacks. Others argue that the sharing of significant amounts of private sector data with the nation's fusion centers will do little to increase security as crucial pieces of terrorism-related information will not be discernible due to being included in databases containing large quantities of irrelevant information. These homeland security observers suggest that the possibility of civil liberty abuses of private sector data residing in a state's fusion center far outweighs the possible benefits that may occur when combining private sector data with other suspected terrorism-related information.

3e. Enhance Public Sector Outreach. Some respondent fusion centers had a relatively pro-active public outreach strategy that included a website, brochures and billboards, and/or a 1-800 "tip" line that encouraged the public to call into the center directly. More often, fusion centers had minimal level of interaction with the public by design[173] and due largely to resource constraints. While not violating the precept that "one size does not fit all fusion centers," it could be argued that, if resources allow, centers should be encouraged to have a public message and image consistent with their public mission. Public support and understanding of what these centers can and cannot do may be essential to their long-term viability. Moreover, the law enforcement elements of fusion centers are responsible for knowing their communities and being able to spot anomalies. Public outreach can facilitate calls into fusion center tip lines when they witness behavior that "just does not seem right."

Pros and Cons. Arguments against this option are likely to be largely resource-based. Centers with fewer personnel do not have the necessary staff to operate these programs, for example, a phone bank necessary for a tip line. If the federal government is considering requiring such outreach as a condition of accepting funds, it may need to provide additional funds, and/or re-programming of existing funds. Arguments in favor of this option include a fundamental belief that these centers serve a public mission and should be not perceived as secret or clandestine entities that are spying on law-abiding citizens. If the centers do not define themselves to the public, they may be defined by other groups who may not necessarily have primary source knowledge about the center and its activities.

---

[173] This was sometimes due to a general law enforcement approach when dealing with sensitive issues - in a few cases, it was due to some of the resources or partners with which the center was collocated (e.g., an FBI field office).

3f. Additional Training for SLT Cleared Personnel. Some may argue that clearing SLT personnel, which remains an obstacle to effective information sharing, (Option 6e) without providing them training on how to handle classified intelligence and how to use it without disclosing sensitive information to their staffs may be unfair and ill-advised. Congress may wish to consider funding additional intelligence training for the SLT personnel assigned to fusion centers. It may also be possible for the federal agency detailees at fusion centers to assist with this process. Congress may wish to consider urging DHS, the FBI, and other agencies with detailees at fusion centers to train their staff to assist fusion center leadership with using classified intelligence and tasking personnel based on threat information, without divulging classified information.

Pros and Cons. Arguments in favor of such a training program include that it may help facilitate necessary information sharing, while ensuring classified information remains secure. However, federal agencies may reject the idea of having field personnel assisting in such an effort and may wish to retain such authority at headquarters.

Option 4: Build Additional Linkages to the Federal Intelligence Community

DNI Michael McConnell's "Focus Area 5: Accelerate Information Sharing," in the *100 Day Plan for Integration and Collaboration*, stipulated, "The Plan includes objectives related to enhancing information sharing within the IC as well as the formalization of fusion centers that are in the process of being developed."[174] Formalization and linkages between the fusion centers and the federal intelligence community could have many interpretations and concrete manifestations. As outlined above, should Congress determine it wishes to take action on this option, a range of possible legislative tools are available, as discussed below.

4a. Formalizing, Creating a Statutory Basis For, and Strengthening the Interagency Threat Assessment Coordination Group. The concept of the Interagency Threat Assessment Coordination Group (ITACG) was first raised in November 2006 in the PM-ISE Implementation Plan, and then subsequently in January 2007 in S. 4., the "Improving America's Security By Implementing Unfinished Recommendations of the 9/11Commission Act" of 2007. Under the terms of the Act, the ITACG, which has been alternatively called the Federal Coordination Group, is intended to "... facilitate the production of federally coordinated products derived from the information within the scope of the (ISE)."[175] Since the establishment of the Intelligence Community there has been little reason or mandate for federal Intelligence Community agencies to have direct or sustained interaction with state and local law enforcement and public safety personnel.[176] What

---

[174] See Office of the Director of National Intelligence, *100 Day Plan for INTEGRATION and COLLABORATION,* p. 9.

[175] See S. 4.RS, Section 131 (b).

[176] Pursuant to EO 12333, *United States Intelligence Activities* (1981), the Central (continued...)

little interaction there was, generally took place between the FBI, a statutory member of the Intelligence Community, and state and local law enforcement entities. It could be argued that the nature of the threat today requires a broader range of interaction. In 2007, the executive branch established the ITACG and the organization was placed a the National Counter Terrorism Center (NCTC). To date few state employees are assigned to the center and most fusion center leaders were unaware of the organization or its mission to provide timely and relevant information to state and local homeland security entities.

Pros and Cons. The arguments against the ITACG, as currently envisioned in S. 4, might include (1) the name itself is misleading, as the group will be unlikely to engage in formal "threat assessment" analysis while at the NCTC, (2) security concerns — back channel and un-authorized communications between state and local representatives to the ITACG could undermine existing intelligence dissemination channels and further complicate the cohesiveness of federal threat assessments to state and local consumers, and (3) the detailing of a handful of state and local personnel to the burgeoning NCTC, while useful, may not be enough personnel to have a substantial impact.

Alternatively, one of the primary arguments in favor of such a center include a recognition of the importance of cross-training and mutual learning. It is sometimes the case that federal intelligence officials and state intelligence officials speak past one another because they each have a limited understanding of respective consumer demands, use different terms and standards, and the don't always recognize the inherent limitations of intelligence. By participating in the production of federally coordinated products at the national level, it could be argued, state and local fusion center personnel will learn about the volumes, specificity, and inherent limitations of the numerous "INTS"[177] collected by the Intelligence Community. Moreover, through interaction with state and local fusion center personnel, federal Intelligence Community officials will learn what is most valuable to state and local personnel, and as such, will be better prepared to create products tailored to their needs.

4b. Intelligence Analyst Exchange — Fusion Centers and NCTC Directorate of Intelligence. While the proposed ITACG would work on developing federally coordinated intelligence products for dissemination to state and local fusion centers for further dissemination, ITACG members are unlikely to be engaged in formal analytical threat assessments. It could be argued that further

---

[176] (...continued)
Intelligence Agency is prohibited from performing any "internal security" functions [1.8(c)]. However, agencies within the Intelligence Community are authorized to "Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities...." [2.6(c)]. Executive Order 12333 is currently being re-written. See Katherine Shrader, "Intel Chief Changing 1981 Security Order," in *MiamiHerald.com*, June 12, 2007, (accessed June 14, 2007).

[177] "INTS" refers to intelligence collection disciplines, for more information see FBI, "INTS the Intelligence Collection Disciplines," available from [http://www.fbi.gov/intelligence/di_ints.htm], accessed on June 27, 2007.

analytical cross-training could be achieved through significantly increasing state fusion center intelligence analysts who are not federal employees to the NCTC's ITACG or Directorate of Intelligence, and offering NCTC analysts an opportunity to work at a fusion center. Congress may wish to consider enhancing support for the ITACG's efforts to enhance information exchange with state and regional fusion centers and facilitate analytical cross-training with state and local representatives detailed to the organization.

Pros and Cons. One central argument against such an exchange is that there may be limited utility. If analysis is a discipline that has at its core a fundamental set of skills, including, but limited to, critical thinking, hypothesis generation and testing, written and oral communication skills, and an ability to ascertain salient trends from voluminous data sets, why does it matter if these skills are exercised at the state or federal level? Furthermore, there are very few fusion centers and/or public safety agencies at the state and local level with the resources and existing capacity for this type of strategic analytical assessment. Another argument against such an option is that fusion center analysts and NCTC terrorism threat analysts, arguably, serve different consumers and, as result, do not necessarily need to understand one another's positions. Arguments in favor of such an option might include that the NCTC is a client of the fusion centers, and the fusion centers are a client for the NCTC's Directorate of Intelligence. As a result, "walking a mile" in your client's shoes can help you understand what is valuable to them. Another argument in favor of such integration could be that threat analysis at the federal level may be more well-developed than at some fusion centers, and cross-training may be very instructive for fusion center intelligence analysts who could also take advantage of other Federal Intelligence Community analytical training session while detailed to Washington, DC.

4c. Draft a National Intelligence Estimate (NIE) Concerning the Potential Nexus Between Criminal Activity and Terrorism. It is an underlying assumption, supported by some terrorist cases within the United States, that some terrorists have engaged in criminal activity or terrorism precursor crimes, to support their activities.[178] One way to prevent terrorism is, therefore, to use all existing law enforcement tools aggressively. Fusion centers can assist law enforcement agencies in directing their resources to areas of greatest threat. However, as mentioned above, one can reasonably question if sophisticated terrorists, those who have received formal terrorism training from established international groups and may be planning catastrophic attacks, engage in criminal activity prior to, and in support of, a terrorist attack. Will following all criminal leads and terrorism tips lead to the disruption of sophisticated terrorist plots?

Should such an NIE not exist, it may be useful to draft one focused on the nexus between terrorism and crime. The DNI's National Intelligence Council could draft it and potential clients might include the Homeland Security Advisory Council, National Security Council, all members of the Intelligence Community, *and* state and regional fusion center leaders. Importantly, research and analysis for the report might

---

[178] See CRS Report RL34014, *Terrorist Precursor Crimes: Issues and Options for Congress*, by Siobhan O'Neil.

incorporate input from the fusion centers to determine the extent to which criminal cases in the United States demonstrate meaningful linkage between precursor criminal activity and terrorist activity. Such data sets could be compared and contrasted to the activities of terrorist groups overseas to determine any commonalities. Any such findings or trends overseas could be applied to the domestic arena, through fusion centers, to align protective resources accordingly.

Pros and Cons. Arguments against such an option might include the hypothesis that existing cases in the United States have already demonstrated a link between terrorism, at least with respect to "aspirational" terrorist groups, and crime. Therefore, there is no need for a specific NIE on the subject, as it would require extensive resources needed elsewhere. Arguments in favor of such an option might include the reasoning that if such a study has not been done, it represents an example of how international trends may inform our national counterterrorism efforts, which include, in part, the contributions of a national network of fusion centers. Furthermore, such an NIE would provide fusion centers with specific trends and potential threats that they could be used to create their own collection requirements as well as enhance their strategic understanding of potential terrorism precursor crimes.

4d. Enhance Mechanisms for Fusion Centers to Task the IC for Information and Receive "Feedback". Currently, fusion centers are limited to going through a relatively slow "request for information" process in order to acquire information tailored to their needs from the federal Intelligence Community. If there is a movement, as DNI McConnell stated, to formalize information sharing with fusion centers, which implies a bi-directional flow of information, there will be a need to develop a robust feedback loop where information shared is assessed and requests for information are handled expeditiously. While not all respondent fusion centers had developed intelligence collection requirements, some not only developed requirements but had collection plans designed to fill those requirements. For example, some fusion centers might ask, how might a simultaneous al Qaeda attack manifest itself in fusion center areas of responsibility, or why might fusion centers be more concerned with thefts of chlorine gas than diesel fuel? Some of this general information reaches fusion centers now, although many argue that federal agencies are still not as proactive and sufficiently wide in scope in what they choose to share with SLT agencies, but it is the follow-up requests that are not met in a timely fashion.

Respondent fusion centers often indicated that information they provided to the federal Intelligence Community, largely through the FBI or DHS went into a "black box," with little feedback as to the value of the information or how it may have been used. Frequently, fusion centers are told that they can't receive follow up information because it is part of an open investigation. Fusion centers are often in a position of not knowing if the information they passed was noteworthy or worthless. They don't know if they should be actively looking for similar information to pass onto the federal community. Moreover, the lack of feedback creates resentment towards federal agencies. State and regional officials reported being further disheartened to learn that locally gathered information they provided to DHS for risk assessment and subsequent grant allocations, was not used in any

systematic and meaningful manner.[179] It is important to note that the lack of feedback and forthcoming information from the federal government is frequently cited as one of the predominate reasons many fusion centers were established initially. Critics might ask, if fusion centers do not have access to feedback, can they ever expect to fully participate in the intelligence cycle and achieve true fusion?

Two bills pending before Congress, S. 4 and H.R. 1, include language, under the sub-title "Homeland Security Information Sharing — Establishment of Business Practices," that would require the Secretary of DHS to "...develop mechanisms to provide (analytical and operational) feedback regarding the analysis and utility of information provided by any entity of state, local or tribal governments or the private sector that gathers such information and provides such information to the Department."

Pros and Cons. An argument against enhancing the feedback loop would include what some might view as a reasonable amount of time for the federal government to respond to fusion center requests. Some fusion centers, as a result of collocation with the FBI or having federal detailess integrated into their centers, might get fairly rapid responses to certain requests for information. However, even some fusion centers with established relationships with FBI JTTFs and FIGs found the FBI still held tightly to certain sets of ongoing case data. An argument in support of such an option, would be if the nation is truly going to use fusion centers as a national network to prevent and respond to man-made and natural disasters, without a timely and effective information sharing and feedback mechanism practiced daily, in times of crisis, the network may prove ineffective.

4e. Establish a Mechanism for Fusion Centers to Have Input into the NIPF. The National Intelligence Priorities Framework (NIPF) outlines the process and results for determining where intelligence assets are directed against prioritized threats. As one would expect, intelligence priorities are linked to assessments of threats to national and homeland security. Yet, today there are few direct mechanisms which allow fusion centers, individually or collectively, to provide their assessments of threats facing their communities into the NIPF.

Pros and Cons. Arguments against this might include the perspective that unless it is a national trend which presupposes a collective sense of existing fusion centers, a threat does not belong in the *national* (emphasis added) Intelligence Priorities framework. One argument in favor of such input could be that the trends being seen at the state and local fusion center level may represent national trends, and/or may include trends not yet identified by federal agencies, even if there is no "national fusion center" currently in existence that integrates all the trends being seen by individuals centers.

---

[179] See CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues and Options for Congress*, by Todd Masse, John Rollins, and Siobhan O'Neil.

4f. Civil Liberties and Privacy Protection — A Role for the IRTPA-Established Privacy and Civil Liberties Oversight Board. While fusion centers were created by state and local governments, with participation and support from federal entities, at what point, if at all, does the federal government become responsible for privacy and civil liberties issues associated with fusion center activities within the states? Where does the federal responsibility to protect civil liberties and privacy stop and where does state responsibility to protect these social goods begin?

It could be argued the more federal financial and human resources provided to the centers, the more the centers are perceived as hybrid federal-state entities. Therefore, the federal government could be *perceived* as being partly responsible for any potential violations of privacy or civil liberties. When Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), it established the Privacy and Civil Liberties Oversight Board to, among other functions, "...review the implementation of laws, regulations and executive branch policies related to efforts to protect the nation from terrorism including the implementation of information sharing guidelines...."[180] If fusion centers are to become true partnerships, it could be argued, that there is shared responsibility to protect civil liberties. In terms of the modalities of the Oversight Board's role, it might work with state agency general counsels to ensure that the fusion centers have requisite policies and practices in place consistent with the Fusion Center Guidelines. Moreover, the Oversight Board might assist in designing an oversight or inspection regime for privacy and civil liberties protection at fusion centers.

Pros and Cons. Arguments against this option might include a belief that as fusion centers are creations of state and regional communities, the federal government has minimal responsibility to exercise oversight with respect to them. Some might argue that legally, the federal government has no right to direct fusion centers on protection of privacy and civil liberties. With respect to privacy rights, it might also be argued that the differing standards for privacy across states would complicate any effort to implement a consistent approach in this area. Arguments in favor of this option might include the claim that even if the federal role in exercising oversight of fusion centers is limited, federal financial and human resources support, as well as support for formalization of the fusion center, requires some level of civil liberties oversight. Some might argue, the current voluntary implementation of civil liberties and privacy protection may be insufficient. Has the federal government conducted audits of fusion centers to determine if they are in compliance with even the voluntary standards as set out in the Fusion Center Guidelines? Moreover, it might be argued that without federal oversight, litigation is likely to serve as the only significant oversight mechanism. Litigation, however, may not necessarily be the most effective oversight tool, due to the length of time it takes for the judicial system to adjudicate such cases. Moreover, by the time an issue has made its way into the courts, there is likely to be considerable skepticism amongst the public regarding fusion center activities.

---

[180] See IRTPA, Sec. 1061, codified at 5 U.S.C. 601 Note.

4g. Create a Statutory Basis For an Intelligence "Confidence" Ranking System for All Federal Intelligence Products. In at least two reported instances, federal threat information reportedly provided to state and local fusion centers and/or state/local officials manifested competing assessments of source reliability and validity and, by extension, the nature of the threat. In the two incidents, which took place in Boston in January 2005 and in New York City in October 2005, the FBI and DHS provided local officials with competing assessments of source reliability and/or the urgency of the threat.[181] Federal officials have since testified that coordination mechanisms have been put in place to prevent such future occurrences.[182] However, in order to assist state and local fusion centers to determine how imminent and/or valid a potential threat may be, Congress may wish to consider the creation of a universal confidence ranking for federally produced intelligence products that would rank an agency's confidence in the reliability of the sources — reflecting the source's reporting history and corroboration with other intelligence sources, etc.

To some extent, the failures associated with certain elements of pre-war intelligence on Iraq have served as a catalyst for an intelligence confidence and transparency initiative underway at the national level and with respect to National Intelligence Estimates. Thomas Fingar, Deputy DNI for Analysis, stated a recognition of the need to "show(ing) our homework — greater transparency about sources, which allow analysts to better assess the quality of intelligence reporting."[183] Former Deputy Director of the CIA's Directorate of Intelligence stated in a speech to all CIA analysts "... that when you are 'calling it as you see it', you must give the policymaker full transparency into your confidence in the judgments you are making."[184] An important question concerning these recognitions, however, is the extent to which this confidence system is formal, and is being extended into products and judgements regularly provided to fusion centers. Congress may wish to consider oversight hearings to determine the progress of this initiative as it pertains to fusion centers.

Pros and Cons. A credibility ranking system might reduce the need to include sources and methods information in intelligence products, thus making the creation of declassified and "less classified" versions of intelligence products easier. Such a ranking would provide state and regional fusion centers better information to use in making informed decisions about the threat to their communities and related responses. An argument against this option suggests it may be difficult to get multiple federal intelligence and law enforcement agencies to agree on common

---

[181] Lara Jakes Jordan, "Bogus Boston Terror Tip Highlighted Information-Sharing Woes, Ridge Says," in *Associated Press*, January 28, 2005.

[182] See transcript of John Pistole, Deputy FBI Director, and Charles Allen, DHS Chief Intelligence Officer, Before the Senate Select Committee on Intelligence, January 25, 2007.

[183] See Maura Reynolds, "Intel Office Gives Dissenters Their Due," in *Los Angeles Times*, April 14, 2006.

[184] See DDI's State of Analysis Speech, All Hands Meeting, CIA Auditorium, Feb 11, 2004. Available at [http://www.fas.org/irp/cia/product/021104miscik.pdf] (accessed June 20, 2007).

"credibility" criteria. Getting consensus on assigning a particular ranking to a intelligence product could potentially be a lengthy process that could potentially delay intelligence dissemination. On the occasion that one or more agencies disagree with the majority consensus, a system for "line-item" analytic comments may be necessary (as is currently utilized for National Intelligence Estimates). It should also be noted, that the credibility ranking system described above is unlikely to have a positive impact on state and regional fusion center analysis and assessment unless it is preceded by training on intelligence, related terminology, the intelligence cycle, etc. to give context to the system.

Option 5: Consider Structural Issues

As mentioned throughout this report, there is no "cookie cutter" approach to fusion centers. Although the centers may all have some core functions, the financial and personnel resources they have to dedicate to those functions differ widely. Structurally, the continued development of the fusion center concept could progress along any of the following, albeit non-exhaustive, paths. Should Congress determine it wishes to take action on this option, a range of possible legislative tools are available that might influence that path of development, as discussed below.

5a. Support the Current Path of Development. Under the current path of development, states and localities continue to make decisions about the number of fusion centers. There is little to no federal input into these independent decisions, as the centers are created and largely funded by the states and localities. This has reportedly resulted in several seemingly unusual homeland security purchases and funding decisions according to fusion center officials who noted the creation of competing fusion centers in some states.

Pros and Cons. An argument in favor of this option is the position that it would respect states rights and the ability of states and localities to make independent determinations about the structure of fusion centers that best fits their needs. An argument against this option suggests the increasingly complexity, from a federal perspective, of funding numerous fusion centers within one state. A proliferating amount of fusion centers in a single state can lead to competition for resources that may lead to an allocation of existing funds that does not necessarily best advance the fusion function.

5b. Support the Designation of One Lead Fusion Center Per State. Under this option, the state's Homeland Security Advisor, acting on behalf of the governor, might dedicate one fusion center as being the lead center for the state.[185] Federal financial resources could be provided to that center, which would have the ability, acting through the state Administrative Agency, to re-allocate a portion of those funds to "satellite" fusion centers across the state. As mentioned earlier in the report, DHS and DOJ have requested that each state governor designate one state

---

[185] The PM-ISE *Implementation Plan* (November 2006, p. 119) included as part of its "PM Recommendations and Summary of Actions," that "DOJ and DHS will work with Governors ...to designate a single fusion center to serve as the statewide or regional hub to interface with the Federal government."

fusion center as the main interface for exchanging terrorism and homeland security information.

Pros and Cons. Arguments in favor of this option might include the belief held by some fusion center respondents that the competition for limited federal resources does not serve fusion centers well. That is, particularly if there are relatively few highly qualified intelligence analysts, having them at one central location where they have easiest access to the flow of information coming into the center may best serve the interests of fusion centers. Arguments against this option may include that fusion centers are essentially state and local entities, and as such, they should be designed in whatever configuration, to include multiple centers if desired, if that is determined to serve the state or locality's interests. For example, some large states have several large cities and having one central fusion center serve as the recipient of federal grants might undermine "satellite" fusion center operations.

5c. Expand the FBI FIGs to be the Federal Strategic Analysis Fusion Centers. Although provocative and radical, fusion center critics might argue that fusion centers are superfluous insofar as the primary federal benefit they seek to provide is prevention of manmade (terrorist) attacks (a traditional federal agency role) and/or destabilizing crime (gangs, narcotics, etc. — both a federal and SLT responsibility). Those who subscribe to this school might argue that state and regional fusion centers could be eliminated and federal agencies take over all the functions those centers once performed, with intelligence and counterterrorism-related work going to the FBI, and the all-hazards functions adopted by some fusion centers turned over to FEMA or the state/local agencies that traditionally handle natural disasters. The counter to this argument is that a changed threat environment requires *non-traditional* thinking — designed to prevent and respond to terrorist attacks and respond efficiently and effectively to substantial natural disasters. Nevertheless, the argument that fusion centers may represent an organizational solution to a functional information sharing and analysis problem can still be made.

A less radical, albeit still drastic, version of this option would suggest that the FBI take over all strategic analysis and assessment roles and that state and regional fusion centers focus solely on tactical analysis of criminal intelligence. Under this option, the FBI's Field Intelligence Groups (FIGs), whose primary purpose is to manage the FBI's intelligence process at each of the 56 FBI field offices, would assume a broader set of responsibilities. One version of this option would have the FIGs conducting this analysis, using FBI analysts, to be shared with SLT agencies. Another approach would have SLT personnel previously assigned to fusion centers be re-detailed to the FIGs to assist with the analytic process, although that process would be run and directed by the FIG. Either way, the FBI might be able to conduct the types of analyses that could assist state and local law enforcement, public safety, and private sector potentially to direct their protective resources into the areas of greatest criminal and homeland security threats *if* the FBI had:

- Direct access to all the state and local criminal intelligence and information that fusion centers have.

- Established relationships with even rural law enforcement personnel, private sector personnel, and other related homeland security stakeholders.

- Information systems which could facilitate the sharing and analysis of unclassified and classified information across all homeland security stakeholders in the country in a timely and effective manner.

This option does not presuppose that existing state and local fusion centers would be supplanted. However, federal financial resources could be re-directed toward the establishment of state-wide intelligence systems that are interoperable and to which the FBI FIGs would have direct access as an input into strategic analysis. Relieved of the strategic analysis burden, fusion centers could focus on tactical analysis in support of constituent member or fusion center cases and/or situational awareness.

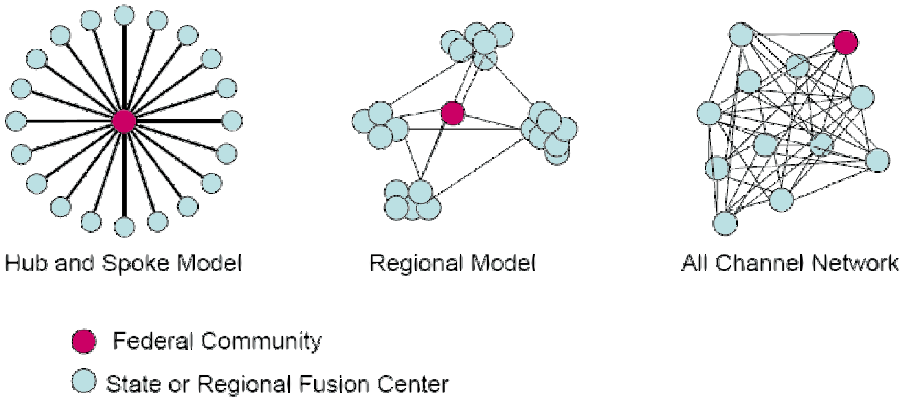
Pros and Cons. Arguments against expanding the role of the FIG relative to fusion centers might find that it represents a thought process that is part of the problem — that is, that homeland security is essentially a federal function, with a minimalist role for state and local law enforcement and public safety personnel. Such an approach might marginalize the important role that state and local homeland security stakeholders can play. It may also result in the failure to fully utilize the resources and institutional knowledge of SLT agencies, the stakeholders who know their own communities more intimately than any federal agency. Moreover, it could also be argued that the FBI is being asked to do so much in the post-9/11 world — to be the foremost counterterrorism and counter-criminal organization in the United States — that this somewhat expanded role may be asking too much. Lastly, from an analytic perspective, tactical and strategic analysis are mutually supportive and it may not be prudent to separate the two.

Arguments in favor of this option might find that such a role for the FBI does not involve supplanting existing fusion centers. It would merely federalize the strategic analytic function, one that many fusion centers have difficulty dedicating personnel to because their clients do not necessarily demand these types of products. Lastly, it is not a great expansion of FBI responsibilities, it only involves analysis of an enhanced set of raw data that is relatively under developed due to the nascency of state-wide criminal intelligence systems. State-run emergency management agencies or the fusion centers in cooperation with these agencies would continue to respond to natural disasters as the FBI fulfills its traditional investigative mission.

5d. Establishment of a National Fusion Center Representative Organization. Today, there are more than 40 plus fusion centers operating, largely independently, around the country. It can be argued that the next fusion-related development should be "2nd generation fusion" or "fusion of the fusion centers." Informally, this has started to happen to some degree. Post-9/11 demands for increased domestic security served as a catalyst for some state fusion centers to collaborate with each other to facilitate the flow of information and intelligence. The means and the ends of that collaboration are important. First, the means - at times, these informal center-to-center or more formalized regional group relationships have been used to share threat information specific to investigating a past or ongoing

incident of concern.[186] To achieve the next step in fusion center collaboration, from ad hoc relationships to a more formalized, structured relationship between fusion centers that would create a representative voice to address mission and resource related issues with the federal government, there are several organizational network models that could emerge, as well as a hybrid of several models:

Figure 1. Organizational Network Models



Source: CRS-generated graphic.

It is important to note that the depictions in **Figure 1** represent "pure" theoretical models.[187] Elements of these aggregate models exist today, although the models could be formally adopted in an effort to bring more structure to the existing fusion center network structure. For example, all the fusion centers interviewed for this report have some direct linkages with other fusion centers, although an individual center may not have established links with every other center in the country, nor are those links of the same strength. It is also common for fusion centers to have stronger links and more constant contact with nearby fusion centers or those centers at similar levels of maturation. To the former point, there are examples where fusion centers in a particular area have set up regional fusion center coalitions, like Southern Shield in the southeast,[188] to facilitate information sharing. Each option has its own advantages and disadvantages. Moreover, like fusion centers themselves, it is not clear that one model would work for all stakeholders involved in the network. In reality, any fusion center configuration is likely to be a hybrid of some or all of the models represented above. However, some homeland security observers

---

[186] Interview with fusion center leader, May 22, 2007.

[187] A hub and spoke model consists of multiple nodes (fusion centers) that are all connected to same central node (a national fusion center or other coordination group). A regional network includes regional groupings of nodes (fusion centers) - with/or without a central node (a national fusion center, etc.) connected with each grouping. An all channel network has each individual node (fusion center) directly linked to every other individual node (fusion center) - with/or without a central node (national fusion center, etc).

[188] Georgia Bureau of Investigation, *Investigative Division Annual Report 2005*, available from [http://www.ganet.org/gbi/05annual/Investigative_FY05.pdf], accessed on June 15, 2007.

argue that significant success in maturing a national fusion center constellation may be assisted by the creation of nation fusion center representative entity that provides the federal government prioritized mission and resource issues of interest.

Second, the ends — an often stated concern by state homeland security leaders is a lack of understanding how the federal government prioritizes funding, personnel, and technical support provided to the nation's fusion centers. Conversely, many homeland security observers note that federal government leadership has difficulty in responding to the needs of the fifty state fusion centers in a prioritized and logical manner. To facilitate a more comprehensive approach to putting forth the needs of state fusion centers in a given region, some state leaders have established regional fusion center representative organizations.

At present individual state fusion centers request services and support from DHS that are relevant only to the organization's operations. It is the perception of fusion center leaders that DHS responds to the needs of a single center without the consideration of the priority of the request with respect to the needs of others centers that may be in locations deemed higher at risk, or the needs of all of the nation's fusion centers. A coordinated national or regional representative fusion center organization that can propose to the federal government prioritized common issues of concern may assist DHS and FBI submit, manage, and allocate fusion centers budgets based on strategy rather than the perceived need by a single center.

Pros and Cons. An argument in favor of the establishment of national fusion center representative organization entails increasing the nation's contextual understanding of threats and vulnerabilities through increased collaboration by state fusion centers. Such an organization may assist the federal government in ascertaining the risks to the nation and understanding the resources needed to support the federal-state information sharing environment. An argument against such a structure is the possibility of the inadvertent creation of a "group-think" environment whereby centers, in an effort to support unity of effort and collaboration, may compromise their independent analysis of risks to the region in favor of supporting the representative organization.

5e. Move Toward Regional Fusion Centers. A second option for addressing the need for 2nd generation fusion is the creation of regional fusion centers to coordinate disparate fusion efforts at the state and regional level. This option is likely to be supported by those homeland security observers who question the viability of each state having its own homeland security fusion center (or several in some cases). There are some indications that federal intelligence community agencies are already considering developing a regional architecture to promote information sharing.[189] Under this option, fusion centers could move to a regional model based on any number of federal regional designations (HIDTA, FBI FIG, FEMA, Drug Enforcement Agency Organized Crime Drug Enforcement Task Forces

[189] Jason Miller, "White House Council Puts Cybersecurity in Focus." FCW.com, July 2, 2007. [http://www.fcw.com/article103121-07-02-07-Web].

etc).[190] Increasing center-to-center and regional collaboration on issues of common concern may help garner support for such a proposal. A regional approach — in the several forms it could take — may help facilitate information sharing, effective resource dispersal, and help transform the current localized, reactive, and tactical approaches to threat analysis to a more proactive and strategic posture. One possible approach to regionalization could be the combining of numerous state fusion centers into a regional homeland security center. Such a strategy may become more popular if there are no large-scale terrorist attacks or disasters in the United States, which result in less homeland security-related funding and a lack of political support to sustain fusion efforts. Such an occurrence may be predicated by the following situations:

- Existing state fusion centers detailing personnel to bordering state organizations thus developing a notional regional network within existing organizations.

- Barring a future terrorist attack or catastrophic natural disaster, the elimination of state fusion centers may lead to the establishment of large regional centers staffed by surrounding state personnel.

- Modeled after numerous existing organizations located throughout the Nation (HIDTAs FBI FIGs [see option 5c above], FEMA), a federal government-led regional fusion center is established in partnership with state employees focused on strategic analysis and/or response efforts in support of federal, state, and local missions.

Pros and Cons. An argument against this option includes the reasoning that by adopting regional fusion centers, the new fusion entities will no longer provide as many benefits to local communities and as such, they will have difficulty maintaining buy-in and detailees from local agencies. An argument for regionalization is the claim that by pooling resources, expanding their scope, and establishing regional spokespersons, regionalization may assist with the resource dilemma and facilitate both more strategic approaches to analysis and effective communication with the federal government.

Option 6: Enhance Information Access and Management

There are numerous measures which Congress might consider in this area to assist fusion centers. Should Congress determine it wishes to take action on this option, a range of possible legislative tools are available that might influence that path of development, as discussed below.

---

[190] FEMA is currently composed of 10 regions, there are 28 High Intensity Drug Trafficking Areas (HIDTAs) and there are nine Organized Crime Drug Enforcement Task Force regions. See [http://www.fema.gov/about/contact/regions.shtm] for the ten FEMA regions, [http://www.whitehousedrugpolicy.gov/hidta/index.html] for the 28 HIDTA areas, and [http://www.usdoj.gov/dea/programs/ocdetf.htm] for nine OCDETF regions. All websites accessed June 12, 2007. The FBI's JTTFs, of which there are over 100, or field offices, of which there are 56, are other regional representations.

6a: Federal Regulations of SLT Criminal Intelligence Systems — 28 CFR, Part 23. As highlighted above, 28 CFR Part 23, the federal regulation which governs state and local criminal intelligence systems, was written, in part, as a response to the domestic intelligence abuses of the late 1960s and early 1970s related to COINTELPRO. While the concerns raised then about civil liberties violations remain demonstrably present today and must be vigilantly guarded against, so too has the threat environment changed. Along with changes in the threat have come substantial technological changes, including the ability to exploit voluminous amounts of commercially available data. As a result, it could be argued that 28 CFR, Part 23 might be revised to include updated information retention time frames and mechanisms to include available technologies.

Pros and Cons. Arguments in favor of such a revision include that a reexamination of 28 CFR Part 23 would potentially result in a new balance being struck between protecting civil liberties and effective and proactive security efforts. Such a revision might also contribute to the creation of national standards for information collection and exchange. Furthermore, changes that address technological advances and the realities of the current threat environment may clarify the limits of how such technologies can be used by fusion centers. An argument against such a revision might include civil liberties advocates being critical of any alterations to 28 CFR Part 23 that may be seen as loosening requirements and/or expanding existing law enforcement powers. Any changes made without SLT consultation and/or that narrow SLT-level leverage are likely to be met with resistence from fusion centers and SLT law enforcement.

6b. Require All Federally Funded Systems to be Interoperable. Peer-to-peer communication has been a priority for the Administration and Congress as demonstrated in the IRTPA instructions to the ISE. Congress may wish to consider further steps to enhance such communication between fusion centers — dubbed by some in the fusion business to be "2nd generation fusion." Congress could consider several initiatives in this area, to include requiring fusion centers and states that wish to use federal funds to purchase information management systems to ensure their systems are able to "speak" to other systems. This would enhance the potential to make connections between disparate data points and reduce information silos at state and/or regional levels. This may limit the number of systems fusion centers can purchases in the short term, but in the long term, such a move is likely to force the companies that sell these systems to work in XML or create the appropriate loaders to translate between XML and its proprietary language.

Pros and Cons. There are several arguments for implementing this option, including the need to ensure federal funds don't contribute to further "silo-ization" of information streams, as well as the potential to encourage more effective information sharing and better data analysis. Arguments against this option may highlight concerns about the immediate limiting impact on systems choices and potential financial costs for state and regional fusion centers and related agencies.

6c. Standardize Reporting Formats. Another option that may enhance peer-to-peer communication among fusion centers and between fusion centers and the federal community is standardized reporting formats. Currently, while there are common "top-down" standardized federal reports, including Intelligence Information

Reports (IIRs), Intelligence Bulletins, and Intelligence Assessments, no such standard set of products exists for "bottom-up" reporting from fusion centers to the federal community.[191] The creation of common lexicon and standards is likely to contribute to this end. DHS has given its roughly 15 fusion center detailees reports officer training to facilitate this effort, but it is clear it needs to be done on a grander scale and in coordination with the FBI and other federal recipients. If this is to be successful, coordination with fusion center staff is likely to be essential to ensure that fusion centers are not overburdened with a multiple reporting formats, required to fill out duplicate copies, and upload through various information systems (Option 6d), thus thwarting effective information sharing. A standardized format will also reinforce efforts to instill the use of a common lexicon and definitions nationally. Such formats should likely include input from state and local law enforcement and fusion centers to ensure consistency and buy-in, and find ways this requirement can fit within existing standard operating procedures rather than creating additional work.

Pros and Cons. A potential impediment associated with this option is the likely difficulty of getting federal and SLT agencies to agree on a standardized report format. Furthermore, it will likely be equally difficult to devise a way to create a common report form and process that does not create additional work for fusion centers. It can be argued that to be effective and efficient, such an option is inextricably tied to the consolidation of federally run information systems (Option 6d, below) and without a serious effort to consolidate information flow between federal and fusion center entities, a standardized reporting format may still be unwieldy. An argument for this option is the assertion that without standardized reporting, the current range of standards and formats being used is likely to impede effective information sharing and analysis, which has been deemed crucial for our nation's homeland security efforts.

6d. Consolidate Federal Information Sharing Systems. Congress might consider compelling federal intelligence and law enforcement agencies to consolidate existing federally owned and operated information sharing systems. Designating a single system as the primary system through which all information from the federal government would be sent to state, local, and tribal agencies may also be an option to consider. Congress may wish to continue to exercise rigorous oversight of the progress the ISE has made toward creating the necessary "policies,

---

[191] According to the ISE Guideline 2, "Fusion centers should continue to maintain and/or develop a capability to support a number of critical counterterrorism, homeland security and homeland defense-related activities, including...(1) state-wide, regional, site-specific, and topical risk assessments, (2) alerts, warnings, notifications, advisories, and bulletins regarding time sensitive or strategic threats, (3) situational awareness reports, and (4) analytical reports regarding incidents or specific threats." See ISE Guideline 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*, pp. 19-20. As indicated throughout this report, a central element missing amongst most fusion centers is a baseline threat assessment. Baseline assessments, arguably, should be a relatively high priority for fusion centers. Standardized product sets, of the type mentioned above, may enhance information sharing across all levels of governments and with the private sector, and could also contribute to the research and drafting of baseline assessments.

procedures, and technologies linking the resources (people, systems, databases, and information) of federal, state, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration."[192]

Pros and Cons. Prioritization and/or consolidation of federally run information systems would likely reduce the stress on fusion centers and enhance the flow of intelligence between SLT and federal agencies. However, it could also be argued that such changes are likely to be opposed by the federal agencies whose respective systems are not promoted as the single information sharing architecture. "Ownership" of intelligence and information systems appears to remain an obstacle in sharing information with sub-federal entities.

6e. Consider Increasing the Number of Cleared SLT Personnel at Fusion Centers. Congress may wish to consider urging the FBI and DHS to increase the number of clearances they provide for state and local personnel, especially those currently assigned to and/or slated to work at state and regional fusion centers. Congress may also wish to examine the classified intelligence reciprocity issue which prevents a holder of a DHS-cleared fusion center, for example, from accessing DOD-origin classified systems and intelligence. While a perennial issue within the federal community, the continued lack of reciprocity creates needless bureaucratic and logistical hurdles that continue to thwart effective information sharing.

Pros and Cons. An argument in favor of this option would be that it allows additional personnel at the centers to receive threat information and direct it to appropriate personnel for action. This may reduce some of the obstacles that currently inhibit the flow of federal intelligence assessments that fusion center analysts can "fuse" with locally focused, grassroots-collected information. With better access to classified information, fusion centers may increase their capacity for "true fusion" by marrying strategic and long-term threat assessments generated by federal agencies with locally focused, grassroots-collected information.

An argument against this option could include the contention that, while seemingly positive, it does nothing to address the over-classification of intelligence, and in fact, could further promulgate a culture of classification. Clearing fusion center personnel, especially management, and not the "boots on the ground" personnel puts the former in a difficult position. They are usually incapable of deploying resources or directing collection based on the classified intelligence they have received. As such, it may be more beneficial to enhance the declassification process — and the capability to create SLT-relevant intelligence products (Option 4a, page 59) — at the federal level then overemphasizing the importance of clearing additional SLT personnel. Furthermore, an increased number of cleared personnel at the state and local level will not be beneficial to fusion centers unless it is accompanied by equipment to receive and store such information, training on how to use intelligence, and guidance on how to identify gaps or generate collection requirements from that intelligence.

---

[192] Program Manager Information Sharing Environment website, available at [http://www.ise.gov/], accessed on June 5, 2007.

6f. Urge Compliance with Intelligence Reform Act and 9/11 Commission Regarding Over-Classification . Congress may wish to examine classification issues and urge more progress on efforts to declassify existing products, as well as produce less sensitive or tear-line versions of classified intelligence reports. This could be done by urging the compliance with the requirements and deadlines laid out in the IRTPA (P.L. 108-458), many of which have not been met. Congress may also wish to consider this and other incentives for facilitating the creation of declassified or "less-classified" versions of intelligence threat reports to ensure fusion centers can receive, store, and utilize threat reporting.

Pros and Cons. A federal government-wide effort to declassify relevant intelligence products could potentially assist SLT agencies and fusion centers to identify potential threats and trends within their respective jurisdictions. Alone, some critics might argue, declassified products based on federal intelligence will not meet the information needs of fusion centers and SLT agencies. Rather, intelligence products need to be created based on SLT information requirements and operational considerations to ensure they are relevant to the recipients. A potential negative tradeoff of a concerted effort to declassify intelligence for fusion centers and SLT agencies might be an increase in the amount of time it takes to get important information from federal agencies to the SLT-level.

Option 7: Create a True Trusted Partnership

In recent years, much has been said about the partnership between SLT agencies, state and regional fusion centers, and federal agencies to tackle homeland security challenges. While there are many agencies, initiatives, and individual leaders who are working to advance the level of cooperation between a wide spectrum of public sector agencies at all levels of government, there are indications that the "partnership" between them is not as strong and dynamic as it is frequently described. It could be argued that the federal government will be hard-pressed to view SLT agencies and entities, like fusion centers, as true partners. Rather, the federal government will likely approach the later as a "consumer" of their work, but not necessarily a common and equal "partner." It is also important to recognize that this tension goes beyond the level of government divide — there is also a significant gap between traditional intelligence and law enforcement agencies (see **Appendix A**), and between first responders and law enforcement.

The relationship between SLT and federal agencies can be tension-filled; they each operate from different historic roles and responsibilities, resources, and jurisdictions. In some locations there appears to be some residual resentment of the FBI and some other federal agencies amongst SLT entities after years of being treated as inferior and an information source — not necessarily as a consumer. On the federal side, there is often a distrust of SLT entities, a concern about the erosion of federal jurisdiction, and, in some cases, a resistence to accepting an enhanced SLT role in some homeland security areas.

Although relationships vary across the country, in some locations the two groups do not have the necessary understanding and familiarity with each other, despite some continued contact (i.e. state and local interaction with the FBI via JTTFs). Several fusion center officials cited their perception about the failure of federal

agencies to understand their needs. In January 2007, Washington, DC, Police Chief Kathy Lanier testified to the cultural differences and lack of understanding between SLT and federal communities:

> the Department of Homeland Security is not a law enforcement agency like the FBI ... is a law enforcement agency.... So it's very difficult for them to understand what my need to know is, if they don't know what it is that I do. If they're not familiar with what I do on a daily basis, what resources I have, and how I can reduce vulnerabilities through the daily activities of more than 4,500 employees here in Washington, D.C. ... So a lot of information doesn't get to me, because they don't believe I have a need to know.... I think it's just a lack of understanding. And this is not in all DHS's fault ... local law enforcement's just as much at fault. The Department of Homeland Security is not completely aware of what our operational capabilities are and how the information, if passed on to us, could be used to reduce the vulnerability.... So information that may be shared with us is not shared with us because they don't think it's something that we can do anything with or that we can use to help reduce that vulnerability.[193]

As mentioned above, this lack of understanding can lead to unrealistic expectations. In talking with state and local officials who are relatively new to the intelligence discipline, it is often apparent that they believe that the federal government knows far more than it tells them, and that the intelligence the "Feds" have is usually clear and specific regarding the "who, what, where and when" of a threat. This is often not the case, but it leads to latent distrust instead of open discussion. As previously stated, the two sides operate using different language and standards. The lanes in the road are often unclear and in some cases there remains a degree of competition between various agencies and levels of government. In short, while there is an enhanced level of trust between the federal and state and local communities, according to some fusion center respondents, they would not necessarily characterize the relationship as a true partnership.

Pros and Cons. Arguments against this option are likely to focus on the difficulty of creating a plan and implementing a strategy for enhancing SLT-federal partnership, something that can be difficult to define and measure in tangible terms. Those who wish to maintain the status quo are unlikely to support such an option. On the other hand, supporters of this option may opine that regardless of logistical challenges, the importance of enhancing the relationships between levels of government and various homeland security stakeholder communities is so essential to post-9/11 U.S. security, that it cannot be ignored.

As outlined above, should Congress determine it wishes to take action on this option, a range of possible legislative tools are available. One concrete manner of working toward this true partnership and mutual understanding is through personnel exchanges.

---

[193] Cathy Lanier, "Intelligence Reform: Federal Bureau of Investigation and Department of Homeland Security," Testimony before a Hearing of the Senate Select Committee on Intelligence, January 25, 2007, reported by Federal News Service, available from [http://www.lexis.com], accessed on June 12, 2007.

Option 7a. Enhance Coordination Efforts Through Personnel Exchanges. It could be argued that the more interaction and detailing of personnel between state and local fusion centers and federal agencies, the better. While periodic conferences are helpful in building relationships, living in your partners environment and understanding the demands and limitations of that environment is essential to building mutual trust and understanding. Potential details of personnel to a Interagency Threat Assessment Coordination Group (Option 4a, page 59) and to the NCTC (Option 4b, page 60), options mentioned above, may be concrete measures which could enhance partnerships and mutual understanding.

Pros and Cons. Additional clarity about each communities' roles, responsibilities, and resources is likely to reduce duplication, clarify the "lanes in the road," influence intelligence sharing selections, and potentially could lead to enhanced coordination. In some cases these issues have been avoided because of sensitivities regarding jurisdictional issues, which could come to a head during such an exercise.

II. Fusion Center Options With No Unique Federal Remedy

There are some issues associated with fusion centers for which there are no unique federal remedies. This is largely due to issues associated with federalism.

State Legal Authorities. There were a number of legal issues discovered in the course of research. Because they involve state law, there is likely no federal remedy, unless constitutional issues are involved, a situation that would have to be assessed on a case-by-case basis.

State Option 1: Add or Revise State Legal Authorities. While acknowledging that the majority of state programs are not recognized by legislation or a governor's executive order, many homeland security observers are concerned that an uncertain funding line coupled with unreasonable mission expectations may lead to the elimination of fusion centers in the future. One near-term priority of fusion center leadership might be to coordinate efforts with the state's homeland security advisor, the governor's office, and state legislators to recognize the center, define its mission, and devote suitable long-term state funding to its operations.

With future federal funding levels uncertain, a situation may be developing that could be detrimental to the future needs of the state. Should a state not recognize or devote dedicated funding to its fusion center, the ability to provide strategic forward-looking threat assessments or tactical operational prevention and response activities may suffer. There are concerns that if the federal government increases funding to fusion centers, mission and administrative conditions may accompany these resources. Such a situation might detract from the state-focused mission and possibly result in the center failing to meet the expectations of state leadership.

State Option 2: Consider Revising Statutory Language Impeding Information Sharing. A number of fusion centers had state laws which had the unintended effect of impeding information sharing. In one instance, a state law made it a Class A misdemeanor if any person knowingly released criminal intelligence information (as defined in statute) to an agency or person other than a criminal justice

agency.[194] According to one fusion center leader,[195] one of the unintended consequences of this law was that any intelligence the fusion center received from the federal community could not be shared directly with any non criminal justice entity or person that may be a target of the threat and/or have resources essential to preventing or preparing for an event.

State Fusion Center Personnel and Management Issues. Research also indicated a number of potentially problematic issues related to state fusion center personnel which, again, do not necessarily have any unique federal remedy. These issues include:

Personnel Option 1: Selection of Fusion Center Leaders. As the fusion centers continue to mature and the security role and functions of the organization attempt to align with the realities of the threat environment, some homeland security observers hypothesize that state leadership may wish to reconsider the attributes required of fusion center leaders. In response to the evolving homeland security environment some centers have started ensuring that the core leadership team of the organization have representative experience and knowledge of the four phases of homeland security: preparation, prevention, response, and recovery. For example, fusion centers that focus on all-hazards may look for leadership that have both criminal and emergency responder experience. Some state homeland security observers are concerned that one implication of a possible significant increase in federal funding to state fusion centers might entail the federal government's desire to be consulted regarding personnel selected by state leadership for positions that are responsible for managing state fusion center funds.

Personnel Option 2: Assignment and Performance of Fusion Center Personnel. One concern often voiced during the interviews with fusion center leadership was the ability to select and manage the personnel assigned to the center. There is a general concern about the quality of detailess. Given resource constraints within partner agencies, fusion center leadership are concerned that those agencies may seek to detail personnel who fail to perform. Considering the immaturity of many of the nation's fusion centers and their need for personnel, centers often unknowingly accept individuals with skills that do not support the mission.

There are also issues regarding clarity of roles and responsibilities. Despite memorandums of understanding (MOU) signed by the fusion centers and the detailing organization, there is often a lack of definitive understanding of the roles and functions the detailee is to undertake in support of the fusion center. With regard to federal agency detailees, this lack of clarity could result in unmet expectations, reduced federal-state coordination, and agency representatives departing the center prior to the conclusion of the assignment. Unlike the lack of specifics of the functions to be performed and the role of the individual in the organization, the MOUs often specify that salary, training, and annual performance reviews will continue to be provided by the parent organization. It is often argued this programmatic arrangement is necessary to quickly detail individuals to the

---

[194] Interview with fusion center leader, March 23, 2007.

[195] Ibid.

organization; however, such a process does not appear conducive to the effective management of individuals detailed to the fusion center.

While it is true that fusion center leaders are on occasion asked about the performance of detailees, many suspect the arrangement does not have a lasting impact on detailee work productivity. Barring dismissal from the center, the organizational relationship limits the leverage a center leader may have in increasing the performance of detailees that may have suspect qualifications or lack of knowledge of the assigned mission. Such an organizational dynamic may negatively affect the center's mission effectiveness and compel center leadership to question the parent organizations commitment to the fusion center.

Personnel Option 3: Employee Performance Metrics. Several fusion center officials mentioned concerns regarding the lack of tools to measure personnel performance. During times of fiscal crisis, which is especially acute in some states, fusion center officials are being pressured to justify their existence in light of other cuts to law enforcement and public services. Without well established entity-wide and personnel specific metrics, fusion centers reported difficulty demonstrating their importance to those officials responsible to budgets and grant allocations. To address this situation, one fusion center was creating their own metrics to evaluate individual performance, based largely on the military performance evaluation system.[196]

Option 4: Sub-State Competition and Lack of Planning. As previously mentioned, many states and municipalities are currently in fiscal crisis. There are numerous agencies and projects competing for limited state budget dollars as well as federal grant resources. Numerous fusion center officials cited the lack of strategic planning for resource distribution within their state. In some states, non-intelligence focused agencies and personnel are responsible for dividing federal grant funds among state/local initiatives. Some fusion center leaders believe a lack of understanding of the role of fusion centers has put the centers at a disadvantage for receiving federal grants from the decision making bodies. In at least one case, a fusion center was told by those making grant distribution decisions that "fusion centers benefitted the federal government, so the federal government should fund them directly" — an indication they did not think the homeland security grant funds should be used to fund that state's fusion center.[197]

Another complaint focuses on the lack of strategic coordination. In some states, regional councils or municipalities themselves can determine what to spend federal homeland security grants on, without proving that such expenditures fit within a strategic state-wide effort to reduce risk. In one state, regional councils that distribute funding choose to fund local fusion centers, even though there was already one established for the state, potentially creating duplication of effort, wasting resources, and stirring competition.[198] One example of poor planning included the authorization by one council for 500 megahertz radios, while another council

---

[196] Interview with regional fusion center leadership, May 1, 2007.

[197] Interview with regional fusion center leadership, May 3, 2007.

[198] Interview with state fusion center leadership, April 25, 2007.

approved and funded ones that were 800 megahertz, thereby perpetuating a lack of interoperability.[199]

Option 5: How States Can Achieve Enhanced Buy-In. Another potential hurdle to fusion center development is creating buy-in at the sub-state level. In many states there are indications that small police departments and public sector agencies are not thoroughly convinced of their fusion center's worth, and if and how the center will benefit them. Creating buy-in is a difficult process. Expanding from a solely counterterrorism focus to an all-crimes approach appears to have helped some fusion centers create buy-in. As previously mentioned, providing investigative resources to small agencies that need them has assisted another in this regard. However, these services are not often "fusion"-related, and thus it begs the question, how can fusion centers convince local law enforcement agencies that they should expend resources and time to working to enhance the fusion process?

Moreover, non-law enforcement agencies are often skeptical about fusion centers. First, all-crimes and counterterrorism-focused centers have a more difficult time than all-hazards centers marketing themselves to public health, environmental protection, fire fighters, etc. These entities tend to have had far less intelligence experience and enjoy a reduced level of comfort with the intelligence cycle than law enforcement. In addition to apprehension with the subject, non-law enforcement public sector agencies are unclear about what role they should play and how to play it. Furthermore, some non-law enforcement fusion center officials complained about what they perceive as conflicting messages from the federal government about the role of agencies like theirs in the fusion process.

---

[199] Ibid.

Appendix A. Philosophies of Intelligence

To better understand the potential philosophical, cultural, and logistical barriers to effective integration of intelligence and information fusion centers with existing federal intelligence and terrorism/crime prevention efforts, it is helpful to examine the different conceptions of intelligence within the federal Intelligence Community and the law enforcement community.

Intelligence Community and Law Enforcement Community Approaches to Intelligence. The absence of a common lexicon between the Federal Intelligence Community and law enforcement intelligence is one area in need of further explanation, as it is manifested in approaches fusion centers take to their work. The majority of fusion centers examined for this report deal with a combination of intelligence, information, and situational awareness. Most centers that described themselves as having a response role or support function for another response-oriented entity were more concerned with situational awareness. However, in a few cases, it was not clear if the fusion center leadership had a thorough understanding of the differences between intelligence and information. This is somewhat understandable: People often use the term *intelligence* interchangeably with *information*, but there is an important distinction.

Intelligence Community Conception of Intelligence. Mark Lowenthal, an expert on intelligence issues, differentiates *intelligence* from *information* in the following way:

> Information is anything that can be known, regardless of how it is discovered. Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs. Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analyzed respond to the needs of policy makers. All intelligence is information; not all information is intelligence.[200]

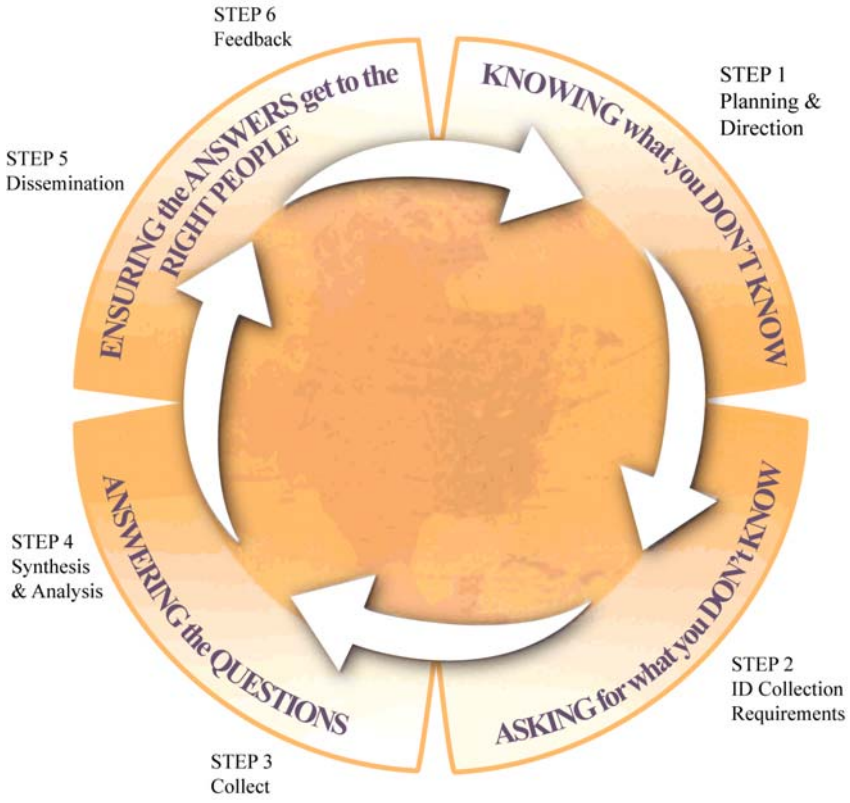
Intelligence is the product of the intelligence cycle (see figure 3 below), a process that begins with Step 1 - planning and direction, which leads to Step 2 - the setting of collection requirements based on threats in the form of questions and identified gaps in existing knowledge, and which is followed by Step 3 - the collection of intelligence based on known gaps. Step 4 includes synthesis and

---

[200] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, Third Edition (Washington DC: CQ Press, 2003). pp.1-2. Lowenthal draws on Sherman Kent's (the "father of intelligence,") conception as intelligence as process, product, and organization. Intelligence as process is a means by which certain types of information are required and requested, collected, analyzed, and disseminated, and as the way in which certain types of covert action are conceived and conducted. Intelligence as product is a product of these processes, that is, as the analyses and intelligence operations themselves. Finally, intelligence as organization can be thought of as the units that carry out the various functions. See Loch K. Johnson and James J. Wirtz, ed., *Strategic Intelligence: Windows into a Secret World, An Anthology* (Los Angeles: Roxbury Publishing Co., 2004), p. 2.

analysis of collected intelligence and results in the creation of an intelligence product, which in Step 5, is disseminated to policymakers and those responsible for taking action based on that analysis. Step 6 is the feedback loop from the customer to evaluate the utility of the product and facilitate another round of the cycle by assisting with Step 1 - planning and direction.

Figure 2: The Intelligence Cycle



Source: CRS — derived from multiple sources.

It is important to explain that there are different definitions of "intelligence," and those used by the fusion centers often differ from the more "pure," conception of "intelligence" outlined immediately above.

Law Enforcement Conception of Intelligence. In law enforcement, the term intelligence has been defined slightly differently than within the halls of federal intelligence agencies engaged in all-source, strategic intelligence. David Carter, a criminal intelligence expert states:

> In the purest sense, intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy direction to law enforcement decision

> makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.[201]

Law enforcement intelligence (LEINT) is thus "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."[202] Carter's definition appears akin to what the Intelligence Community would consider "finished" intelligence — intelligence that has been synthesized and analyzed. One might argue that criminal intelligence, as conceptualized above, is reactive — information becomes intelligence after it is analyzed, as compared to more pure concepts of intelligence, which are more proactive, in that pre-identified intelligence gaps based on policymaker needs are the starting point for intelligence collection. This would be in line with traditional approaches. It could be argued that the Intelligence Community tends to be proactive in dealing with national security matters, while law enforcement in the United States has traditionally been reactive, post-event, and prosecution focused. Some might argue that the use of law enforcement tools such as the enterprise theory of investigation have indeed been proactive in the collection of intelligence, although not necessarily through the formal implementation of the intelligence cycle. Carter believes intelligence can be used for both prevention and planning/resource allocation within law enforcement.

The primary differences, then, between pure or traditional conceptions of intelligence and law enforcement intelligence lie in the following three areas: (1) the predicate for the intelligence activity itself, (2) intelligence clients and consumers, and (3) the legal regimes under which intelligence is collected. Whereas the pure intelligence community uses a known intelligence gap as the starting point for collection, it is less likely that a law enforcement intelligence group will have a developed set of intelligence collection requirements and, as a result, a criminal event or case is the starting point for intelligence collection. With respect to consumers, while the Intelligence Community serves action-oriented officials within the military

---

[201] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*, (Washington, DC: US Department of Justice, Office of Community Oriented Policing Services and Michigan State University, 2004), p. 7.

[202] Ibid, 10. Alternatively, law enforcement *information* can be defined much more broadly. For purposes of the ISE, law enforcement information means "any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or security of our homeland and (B) relevant to a law enforcement mission, including, but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigations or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offender; and victim/witness assistance." See ISE Guideline 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*, p. 13.

and federal intelligence communities, it largely serves the needs of national policymakers. In the law enforcement community, the consumers are largely law enforcement officers investigating a crime or criminal groups, prosecuting attorneys and law enforcement executives seeking to align protective resources. From a legal regime perspective, national intelligence collection, arguably operates under a less restrictive legal regime than law enforcement intelligence, an issues which is largely driven by the subjects of intelligence collection — U.S. persons or non-U.S. persons.

The conceptual differences between these two closely related communities and disciplines has implications for fusion centers. Under which model and legal regime are they operating? As mentioned above, how proactive can the centers be in intelligence collection without violating civil liberties? A lack of clarity on these issues can lead to fusion centers either taking a too conservative or too aggressive approach, either of which undermines their full productivity, and serves as an overall risk to the fusion center concept.

Appendix B. Map of Current and Planned Fusion Centers

Figure 3: Map of Current and Planned Fusion Centers