POLICING TERRORISM REPORT
No.2 September 2007

STATE FUSION CENTER PROCESSES AND PROCEDURES: Best Practices and Recommendations

John Rollins

Timothy Connors
Director
Center for Policing Terrorism

Published by Manhattan Institute

CPT
CENTER FOR POLICING TERRORISM
AT THE MANHATTAN INSTITUTE

About the Authors

JOHN ROLLINS is the lead author of this report. Mr. Rollins is a member of the Library of Congress's Congressional Research Service (CRS), where he serves as a Specialist in Terrorism and International Crime. Prior to joining CRS, he was chief of staff in the Office of Intelligence for the Department of Homeland Security. Mr. Rollins's career includes a variety of analytic, legal, and management positions in the U.S. Army, FBI, CIA, DIA, U.S. Marine Corps, Delta Force, and United Nations. He is a licensed attorney and a graduate of the Senior Executive Fellowship program at Harvard University. He also teaches national security courses at a number of universities. The analysis and opinion contained in this report are solely those of the authors and do not reflect the views of CRS.

TIM CONNORS is director of the Center for Policing Terrorism (CPT) at the Manhattan Institute. He is a graduate of West Point and holds MBA and JD degrees from the University of Notre Dame. Mr. Connors has helped law enforcement agencies across the country develop sound counterterrorism and intelligence policies and practices. He is a career Army officer who is currently assigned to a civil affairs unit in the Army Reserve.

CONTENTS

State Fusion Center Processes and Procedures: Best Practices and Recommendations

John Rollins and Tim Connors

INTRODUCTION

America's radically decentralized law enforcement system—there are more than 17,000 separate police departments in the United States—is both a strength and a weakness. It is a great strength because the police are better attuned to their local communities and are directly accountable to their concerns. But it is also a terrible weakness in the post–September 11 world, where information sharing is key, and the sheer number of agencies often inhibits information sharing.

Fusion centers – state and regional intelligence centers that pool information from multiple jurisdictions – are the primary platforms for improving law enforcement's intelligence-sharing capabilities. In recognition of the importance of fusion centers, President Bush highlighted the work being done in these facilities during a recent speech in which he also called America's 800,000 state and local police "the front line in defeating terror."

Federal agencies are not built to be the eyes and ears of local communities; local law enforcement—with the right training and support—can be. Yet there is still much work to be done in order to fully enlist state and local law enforcement in the war on terror. As Los Angeles police chief William Bratton and Manhattan Institute senior fellow George Kelling wrote last year in a Manhattan Institute Civic Report titled "Policing Terrorism":

> Americans accustomed to television shows such as *24* and *CSI* think that law enforcement has all sorts of intelligence information at its fingertips. This could not be further from the truth. The unfortunate reality is that law enforcement—federal, state, and local—is very far behind the private sector in terms of the ability to use technology to gather, analyze, and disseminate information.… When you rent a car today at many airports, an attendant will come out with a handheld device that enables him to gather all the information he needs on you and the car, send it wirelessly to a main database, and bill your credit card, all within a matter of few seconds. Just imagine what might have happened if the Maryland state trooper who had stopped 9/11 hijacker Ziad S. Jarrah for speeding on September 9, 2001, had had access to that type of technology and had discovered that Jarrah was on the CIA's terrorist watch list.

The 9/11 murderers exploited law enforcement's inability to harness the information systems that are commonly available today. Fusion centers are central to erasing that deficiency. If properly operated, fusion centers will enable law enforcement to harness information and intelligence to better identify, assess, and manage emerging threats to public safety.

Fusion centers represent the front line in spotting the sort of threats that went undetected on that deadly day six years ago. And they are having a real impact. As reporter Judith Miller wrote in the Summer 2007 issue of *City Journal* describing the Los Angeles area fusion center:

> Homeland Security now has an official stationed full-time at L.A.'s crown jewel of "jointness": the Joint Regional Intelligence Center, or "Jay-Rick," which both Bratton and Chertoff hold up as a model for similar fusion centers soon to be operational in more than three dozen U.S. cities…The JRIC's analysts don't conduct investigations; instead, they vet tips and leads—nearly 25 new ones per week—to identify the 1 percent that prove serious…[The Commander of the LAPD's Counter-Terrorism and Criminal Intelligence Bureau Mike] Downing says the LAPD has arrested some 200 American citizens and foreigners with suspected ties to terrorist groups since September 11. At present, he adds, his division has 54 open intelligence cases, involving at least 250 "persons of interest." One of the most celebrated examples of the strategy is the 2005 Torrance case, in which the arrest of two men for robbing a gas station in that city eventually unraveled a militant Islamic plot to attack U.S. military facilities, synagogues, and other places where Jews gather in Los Angeles County.

In this report, the Manhattan Institute's Center for Policing Terrorism (CPT) offers twelve recommendations for establishing new—or enhancing existing—fusion centers. We base these recommendations on a review of current literature, an assessment of existing fusion centers, and interviews with federal, state, and local leaders. Since the resources available to state and local governments are constrained, we have attempted to provide recommendations that we deem to be both necessary components of a well-functioning fusion center and resource-neutral.

It is our hope that the recommendations and information shared in this report will assist municipalities in strengthening the operations of their fusion centers. CPT thanks the members of the New Jersey State Police, the leadership and members of the New Jersey Regional Operations and Intelligence Center (ROIC), and the New Jersey Office of Homeland Security and Preparedness for the opportunity to discuss these recommendations and learn from their experiences. We would also like to thank the leadership of the Naval Postgraduate School Center for Homeland Defense and Security, who greatly informed this effort.

Sincerely,
Tim Connors and John Rollins

STATE FUSION CENTERS IN THE POST-9/11 ENVIRONMENT[1]

> *Our goal is to have a two-way flow where federal, state, and local officials contribute and analyze intelligence information collected at every level. By the end of 2008, we will have intelligence and operations personnel at every major fusion center in the United States.*
>
> —DHS Secretary Michael Chertoff[2]

The 1993 bombing of the World Trade Center in New York precipitated one of the most extensive law enforcement investigations in U.S. history. We came to learn that a small band of Islamists, inspired by Omar Abdel Rahman, the "Blind Sheikh," were behind this despicable act. What followed was a traditional criminal-justice case, in which the crime was investigated and the perpetrators prosecuted in criminal trials. Once these individuals were sent away to prison, the case was concluded.

Analyzed information is the lifeblood of the fusion center.

Law enforcement gave little thought as to why an Egyptian cleric and a group of his followers would do such a thing. Why did they carry out a terror attack here? What did it portend for the future? Did this attack represent an emerging and growing threat to public safety that law enforcement would have to eventually confront? If so, how would law enforcement have to organize to confront these threats?

These are typical questions that an intelligence analyst attempts to answer using the intelligence cycle and other tools that are available in the field. In 1993, "intelligence" was a dirty word in law enforcement. Given a history in the 1960s and 1970s in which police intelligence units all too often violated citizen groups' First Amendment rights, there was a widespread movement to dismantle such capabilities.

As a result, in 2001, law enforcement was not prepared to deal with the looming threat of terrorism. It had a very limited capability to identify these threats, gain understanding, and apply resources to preventing acts of terrorism. Fusion centers are designed to help address these shortcomings.

Defining what a fusion center is and what it does is a seemingly easy—but increasingly challenging—task. In varying levels of functionality, operations centers[3] have existed in state and local governments since the formation of police departments and emergency operations organizations. While the establishment of state operations centers is not a new concept, the permanent, physical, and organizational meshing of numerous entities that have each historically focused on a separate public safety discipline is a new concept. Whether the focus is on activities in preparation for or in response to natural (hurricanes, floods, etc.) or man-made (criminal, terrorist, etc.) incidents, yesterday's operations centers are being subsumed into today's fusion centers. These new organizations are responsible for analyzing and responding to a wide variety of events that may threaten[4] the public safety or the property of a state.

Historically, state leaders have received information[5] from numerous state operations centers that were each exclusively focused on a particular problem area. Typically, these operations centers were only responsible for servicing other state agencies. Although this type of operations center still exists in many states (and major metropolitan cities), the trend, especially since the attacks of 9/11, is to combine a number of these centers into one multifaceted organization, often located in a single facility.

Following this trend, fusion centers are evolving into one-stop shopping organizations that are responsible for analyzing all-hazards threat information, tracking asset location and operational readiness, and issuing reports related to current, emerging, and future threats. At a minimum, the core mission of these post-9/11 fusion centers is to report on information that may affect the security of a given locality. But most go beyond this single purpose and perform other functions as well. For example, fusion centers have the ability to quickly analyze information in support of the immediate and proactive deployment of operational assets and re-

sources, as well as to analyze and report on long-term threats—whether those threats result from the weather, a bird flu, crime, or a potential terrorist attack. Generally speaking, the future of fusion centers will be to provide management and information services across a full spectrum of public safety threats.

The primary responsibility of today's fusion centers is still to ensure that state and local leadership is knowledgeable about current and emerging trends that threaten the security of relevant jurisdictions. But this new generation of operations centers differ from its predecessors in serving a variety of customers – private as well as public. The recipients of fusion center reporting are as vast as the sources of data received by the center: critical infrastructure owners and operators, private-sector entities, federal law enforcement and homeland security partners, public and private health organizations, international partners that collect information on threats to the United States, and numerous others.

Fusion centers have been slow to incorporate private-sector partners. The reasons for this include lack of guidance on which partners should be included, a failure to identify partners based on risk, and perhaps a lack of appreciation of the importance of including the private sector.[6] A good place to start is with a careful study and reasoned application of the National Infrastructure Protection Plan.[7] Fusion center leaders can identify appropriate partners and establish priorities based on the seventeen Sector-Specific Plans identified in Homeland Security Presidential Decision Directive 7 and analyzed in a number of documents sponsored by the Department of Homeland Security. Ideally, this analysis will build upon ongoing efforts in the state to align action plans with these authorities.

The federal government has recognized fusion centers as the information-sharing focal point for most[8] homeland security–related issues.[9] Current federal government support to state fusion centers occurs in the form of detailing of personnel, providing technology and equipment, assisting with security clearance processing (many state and local leaders think that this is an area that needs to improve), and offering training and education courses. It is also widely expected that future DHS funding grants will continue to support the establishment and operation of state fusion centers.[10]

CURRENT BEST PRACTICES AND RECOMMENDATIONS

Hundreds of recommendations exist regarding the establishment and management of fusion centers.[11] However, many of these recommendations are resource-dependent and focused on marginally refining current operations rather than developing a sound organizational foundation resulting in enhanced center capabilities. This document focuses on the strategic organizational issues that form the foundation of a successful fusion center. The twelve fusion center recommendations offered here are broken down into the following areas: establishing, supporting, and operating.

I. Establishing the Fusion Center

Although often viewed as laborious and unexciting, theoretical foundations and administrative functions are crucial to the future success of a fusion center. Therefore, responsible leaders should devote concerted energy to establishing sound fundamental policies. Doing so will help minimize the inevitable friction of multi-agency undertakings, enhance situational awareness of all stakeholders, and ensure that the fusion center contributes to the operational success of the member organizations. In addition, given the numerous public and private sector entities that the fusion center serves, the more participation these entities have in adopting and implementing center practices and procedures, the greater the opportunity for future goodwill and support of state and fusion center mission objectives.

Step 1: Develop an Easily Understood and Universally Recognized Mission Statement

A state fusion center must adopt a mission statement that is linked to and supports the goals and objectives

of the state's governor and his or her administration. Fusion center leaders should include partner agencies and prospective participants in crafting a mission statement and strategic vision for the organization. While the center's leadership should retain the final decision-making authority, a participative approach will enable partner agencies to have a sense of ownership in the organization. The idea is to learn about and manage the expectations that partner agencies bring with them. It is a safe bet that unknown, unfulfilled, or unrealized expectations will be at the root of most disappointments in assessing center performance.

Mission-statement clarity is the key to allowing all parties to understand and support fusion center activities. As such, the mission statement should be easily understood. Given the many competing interests, this can be a difficult proposition. As a rule of thumb, a good place to start is to draft a succinct mission statement that fulfills the expectations of various state leaders (assuming that a state agency, such as the state police, is the lead agency in the fusion center). The resulting draft statement can form the baseline for discussions with partner agencies.

It is important to keep in mind that the final version of the fusion center's mission statement must be relevant for a multi-entity organization. It will therefore be important to avoid language that is commonly associated with an individual agency, such as "law enforcement" or "homeland security." Rather, it is better to articulate a common functionality, such as "receipt, exchange, analysis, and dissemination of information" and to adopt an inclusive operational objective, such as "public safety," "preventing terrorism," or "supporting the operations of partner agencies."

The fusion center's governing committees (see Step 5, below) should review the mission statement on a periodic basis to ensure that it remains relevant and easily understood and that it continues to provide the central organizing principles that effectively mold collective action.

Fusion Center Mission-Statement Examples

New Jersey, Regional Operations and Intelligence Center (ROIC)

"Maintain statewide situational awareness for response to current and future security issues concerning the State of New Jersey. The New Jersey ROIC collects, analyzes, and disseminates criminal intelligence and other information (including but not limited to threat assessment, public safety, law enforcement, public health, social service, and public works) to support the efforts of allied agencies."

Massachusetts, the Commonwealth Fusion Center

"Provide 24 hours a day, 365 days a year, statewide information sharing among local, state, and federal public safety agencies and private sector organizations in order to facilitate the collection, analysis, and dissemination of intelligence relevant to terrorism and public safety."[12]

A fusion center's success depends on organizational focus and meaningful, timely information sharing—not large facilities and substantial funding.

Step 2: Develop Implementing Strategies

A well-understood mission statement enables the development of implementing strategies, as well as identifying those lesser tasks that will ensure overall mission success (e.g., policies and procedures, which are discussed in step 3, below). A comprehensive strategic document will answer the question of how each individual fusion center capability aligns with the center's mission statement. It will also outline

the center's fundamental approach to core functional areas such as crisis preparation and response, maximizing the use of available assets (those available to partner agencies as well as those in the private sector), criminal intelligence processes, and homeland security functions.

This strategic document should provide a big-picture understanding of how the fusion center goes about its business. It will enable the center to compare its current and desired end-state capabilities and develop a road map of the near-term, intermediate, and long-term steps required to reach full fusion center capability.

Like the development of the mission statement, the development of the center's implementing strategies should include a broad number of fusion center partners from as broad a level of seniority as is feasible. While such a process is slow, it is wise in the long run to seek opportunities for participants from multiple agencies to build a sense of pride and ownership in the center.

Once the governor or other appropriate authorities have approved the mission statement and strategy, the center's leadership should brief all members.[13] Leaders should deliver this briefing on an annual basis to ensure that members understand the role of the fusion center in securing the state's safety. Routine dissemination of this information facilitates an understanding of such things as the overall mission, core center functions, supporting capabilities, process improvement plans, and organizational roles.

Step 3: Develop Fusion Center Policies and Procedures

Developing easily understood policies and procedures helps fusion center leaders shape a unique culture and make representatives from multiple participating agencies aware of the collective organizational expectations. As with the mission statement and fusion center strategy, the more involved the various participants are, the greater the likelihood that the policies and procedures will be understood and followed.

As issues addressed in the policies and procedures manuals pertain to the daily operations of the fusion center, leaders may wish to task senior center personnel, who best know the inner workings of the information and operations flow, to lead the development efforts. The collaborative-based recommendations and results should then be presented to the fusion center governance committee (see Step 5, below) for refinement and approval. Policies and procedures should be routinely reviewed and updated using the same collaborative process.

Areas that might be addressed by a formal policy or procedure include:

- Center objectives and goals
- Fusion center chain of command, personnel management, and performance appraisals
- Roles, responsibilities, and authorities of center participants and representative organizations
- Protection of privacy and civil liberties; the requirement as delineated in 28 CFR, part 23 should be addressed specifically[14]
- Information collection, storage, use, tracking, and dissemination
- Operational/information security
- Physical/site security
- Individual and collective training
- Budget formulation and execution

Step 4: Develop a Multiyear Sustainable Budget

A fusion center requires a budget that is comprehensive, sustainable, forward-looking, and, most important, realistic—whether the center is functional or in development. A well-reasoned and sustainable budget will include funds for:

- Facility establishment, maintenance, and upgrades (including information technology hardware, software, and communication tools)
- Current and future employees (common practice for federal and other participating agencies to fund their respective detailees)
- Training and exercise
- Reserves to cover extended operations and unforeseen requirements
- Conferences and professional development
- Morale, welfare, and team building

Currently, the bulk of funding for fusion centers comes from state and local government. Since fusion centers are statewide assets and not exclusive to a particular agency, they should be funded as a separate line item in the state's budget. According to a recent report by the Congressional Research Service:

> 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% to 100% of fusion center budgets, with the average and median percentage of federal funding approximately 31% and 21%, respectively. Thus, it appears that on the whole, fusion centers are predominantly state and locally funded.[15]

Wherever the sources of funding are derived, the authorized budget should align with the mission of the organization and the agreed-upon implementing strategies. Expectations of the state's political and public safety leaders and anticipated customer desires must also be considered in the budget formulation process. Thus, the starting point for forming a budget is establishing or reviewing the center's mission, implementing strategies, and determining leader and customer expectations. The objective of this analysis is to identify and prioritize what needs to be done to accomplish the mission and meet leader and customer expectations.

Once that analysis is completed, sources of funding must be identified. These will include federal government grants, particularly from DHS and DOJ, contributions from sponsoring agencies,[16] nonmonetary contributions from partner agencies (e.g., office space, computers, office equipment), grants and other contributions from nongovernmental organizations,[17] and support from the business community. State government is typically responsible for funding remaining priorities. In light of the state's sponsorship role, budget proposals should be presented to the state's political leaders with funding specifics delineated to show the cause and effect of the budget being approved at differing levels.

It is worth noting that federal government funding is not absolute and unending, so the budget should not become overly reliant upon these monies for future requirements. Federal funds are generally provided for the period requested with no guarantees of future grants. Programs initiated with federal funds will present sustainability risks if the program will not conclude in the time frame specified in the grant. It is prudent to develop alternative funding plans in these cases in advance of a crisis generated by the cessation of federal funding.

As discussed in Steps 7 and 11, below, fusion center budgets and underlying funding proposals are quite often heavily laden with information technology requests. When considering technological purchases, decision makers should avoid the search for silver-bullet solutions. Technology in and of itself cannot solve problems unless it supports the activities of human operators and organizations. It is a general and unfortunate trend that fusion centers have reached for technological solutions before considering organizational design, organizational culture, and fundamental doctrinal approaches. The results can be disastrous—wasted resources, organizational ineffectiveness, low morale, damaged credibility, and even the discontinuation of the program.[18]

In determining the true cost of a technology, decision makers must also consider all the supporting systems and activities that are required in fielding and sustaining it. Examples include end-user training, installation, ongoing maintenance costs, upgrades, and interoperability issues. A sound fusion center budget incorporates these requirements in its funding planning.

II. Supporting the Fusion Center

Step 5: Establish a Governing Structure

The fundamental purpose of a fusion center is to bring multiple agencies together in an environment set up to share and analyze information. Given the multiplicity of organizations involved, an agreed-upon method that ensures unified decision making and oversight is indispensable. The difficulty is in balancing the need for control of contributing agencies with the need for

efficient decision making that guides operations. Too many controls mire center performance in bureaucracy, whereas too few controls increase the risk of harm to a contributing agency.

Governance committees can fulfill the two core management functions for the center: leadership and decision making; and oversight and accountability. They can be established in the form of informal advisory panels or formal boards that have a more directive and specified role over the conduct of the organization. It is also worth considering the appointment of a unified director who would manage routine activities and implement collective decisions and who could report to an executive committee. Two forms of governance committees should be considered: internal and external.

The role of the fusion center is to inform state leadership and prepare, prevent, and respond to emerging and future threats.

1. Internal governance committees are formed by representatives of those entities that rely on the fusion center for services and products. Membership on these committees would include leaders from state agencies and private-sector entities and representatives of other affected agencies that have routine interaction with the fusion center. Examples of the types of governance issues such committees would be well suited to address include development and optimization of fusion center products and services, budget formulation and execution, fusion center mission and vision, tasking the fusion center to analyze specific issues, and reviewing operational processes.

2. External governance committees are composed of individuals or organizations that do not have a formal relationship with the fusion center, do not typically rely on the center's products and services, and are not directly affected by the committee's recommendations or results. These committees provide an "outsider's" review and advice. Membership on these committees might include other state fusion center representatives, recognized fusion center experts, civil rights advocates, and individuals familiar with service-oriented organizations. Examples of the types of governance issues such committees would be well suited to address include civil liberty protections, independent review of controversial or critical decisions, and independent oversight of compliance issues.

Independent oversight is a valuable management function that should be sought and welcomed. Not to create this capacity by intelligent design will likely lead to having an oversight structure imposed in a crisis. While informational and operational security are nonnegotiable priorities, it is in the best interest of the center to have an independent authority validate that the center is operating within constitutional and legal limits and that appropriate accountability actions are taken when mistakes are discovered. Given our traditional political values and a history in which law enforcement's intelligence activities have sometimes been questionable, it is inevitable that fusion center operations will be challenged. Routinely stonewalling such challenges is a mistake; rather, it is better to build the capacity to deal with such challenges so that the public can rest assured that the center is doing the right things. Fusion centers that actively build and maintain this reputation will separate themselves from centers that do not make the effort.

In addition to oversight, most of the recommendations contained in this report would benefit from the establishment of governance committees. Depending on the issues to be addressed and the prospect for successful near-term conclusion of the issue, the establishment of governance committees can be permanent or for a short duration to discuss ad hoc issues. However, standing committees should be designed to provide leadership, facilitate decision making, perform oversight, and ensure accountability

Step 6: Develop a Fusion Center Staffing Plan

Recalling that this report provides recommendations independent of the need to request additional resources, these staffing-plan options assume that the fusion center already has state employees assigned to it. It also assumes that federal, state, local, and private-sector partners that detail representatives to the center will continue to compensate those people. Therefore, adding partner agencies does not result in additional personnel costs.

With that in mind, it is a general rule that more resources are usually better than less. In this regard, the federal government has made significant resources available to populate fusion centers around the country.[20] While this support remains critical, fusion center leaders should demand that such outside support results in staffing the fusion center with high-quality people that possess the right skills. It is a mistake to compromise on quality in order to achieve other goals (e.g., obtaining grants, ensuring participation of a partner agency).

It is better to have fewer people with the needed skills than to have more people who have lesser ability to support the goals of the sponsoring agency or enhance the operations of the center. There are two basic questions that govern personnel decisions: Does this person have the skills that the center needs? Is this person a high-quality performer? A center might look to have all the appropriate representatives when it accepts people with the wrong skills or who lack a solid record of achievement. However, it might actually be less capable than it would be with fewer of the right people.

To avoid such a situation, it is imperative that fusion center leaders determine what skills and how many people are needed to staff the center. This planning should begin with an analysis of the center's mission, implementing strategies, and customer expectations. Then planners should inventory current personnel numbers and skills and compare these to mission requirements. This process is undertaken to identify human-resource gaps in mission capability. Using this fusion center staffing assessment, center leaders can make credible personnel requests to partner agencies.

Required skills can vary, depending on the mission of the fusion center and the needs of the detailing organization. However, expertise in the following general areas is typical for most fusion centers:

- General leadership and management
- Crisis and emergency management
- Disaster management experience relevant to the jurisdiction
- Terrorism and counterterrorism
- Intelligence management, collection, and analysis
- Criminal investigation
- Fire safety and firefighting management
- Health management and food safety
- Information technology

Other planning considerations might include:

- Ratio of fusion center employees to partnering-agency detailees
- Whether fusion center leaders are hired as permanent center employees or drawn from partnering agencies
- Fusion center policies and procedures
- Desire to create an inclusive environment
- Operational reliance on specific detailees
- Whether or not resources accompany the detailee (see Step 7, below)
- Nontraditional representation: owners of critical infrastructure, health-care professionals, academic experts, etc.
- Staff required for routine versus crisis operations
- Positions that require 24/7 presence during non-crisis operations
- Positions that require extended work hours during crisis operations
- Ability to quickly infuse operating personnel during a crisis
- Development of secondary skills for those individuals with attributes not called upon during a specific type of incident

Information sharing comes down to two things: giving you the information you need to make judgments about protecting your communities; and capitalizing in the force-multiplier effect that comes when we work together.

—Robert Mueller, director, Federal Bureau of Investigation[21]

Step 7: Develop Memorandums of Agreement with Partnering Organizations

The model for most fusion centers is a state-led, interagency organization. In some cases, a consortium of agencies provides leadership, but those fusion centers are still fundamentally interagency affairs in which the roles, responsibilities, and authorities of partner agencies need definition. As with other areas, allowing this to occur by happenstance as opposed to intelligent engineering is a mistake. The best method to integrate partner agencies is to use a carefully negotiated memorandum of agreement (MOA).

It is imperative that the MOA and supporting memorandums of understanding (MOU) explicitly reflect the needs of the center and the responsibilities of the partnering agencies. The fusion center and the partnering organization should ensure that the MOAs and MOUs contain the necessary specificity to realize the expectations of all parties and to allow for an environment whereby all members of the center are properly utilized in carrying out their duties to safeguard the state.

For reasons of scarce resources, all too often the organization accepts a partnering agency's offer to place personnel and equipment in the fusion center without a clear understanding of the role and contribution that these individuals or items will make. In many cases, the resulting effect is confusion as to individual responsibilities and how such donated technology enhances the current mission effectiveness.

It is important, when accepting such offers, to articulate how the contribution will enhance existing or planned programs. If the center has taken the time to develop a fusion center staffing plan (see Step 6, above), it will have a good place to start this discussion with potential partners. That discussion can then form the basis of a written MOA. The bottom-line measure of success is to ensure that: (1) people accepted into the organization have their individual roles, responsibilities, and authorities defined; and (2) equipment contributions can be smoothly integrated with existing architecture.

At a minimum, fusion center MOAs should address:

- Personnel assignment criteria; required skill, seniority, shift work
- Specific fusion center role of the detailee (i.e., job description)
  - o Liaison officer with unspecified duties
  - o Operations officer responsible for directing resources and assets
  - o Intelligence analyst responsible for analyzing information and reporting findings
  - o Critical infrastructure specialist
  - o Emergency management specialist
  - o Subject matter expert (e.g., terrorism, WMD, health care)
- Duration of assignment
- Chain of command
- Individual responsibilities to the fusion center and to the detailing agency
- Rules for sharing information with the fusion center and the parent agency
- Rules for safeguarding operational security and intelligence sources and methods
- Funding requirements for the detailed individual(s)
  - o Salary (reimbursable versus no cost)
  - o Living expenses
  - o Transportation
  - o Equipment
    - ▪ Computer
    - ▪ Telephone and cell phone (secure and unsecure)
    - ▪ Portable communication device
- Security clearance considerations

Step 8: Develop Fusion Center Education and Training Programs

Molding people from a multitude of organizations into a cohesive team is perhaps the most significant challenge facing fusion center leaders. Detailees from partner agencies will bring with them the organizational culture, lingo, and practices of that partner agency. Furthermore, detailees will have dual loyalties—to the partner agency and to the fusion center. A rigorous, mission-focused training and education plan will help overcome these potential obstacles.

In order to achieve the desired effect on fusion center cohesiveness, collective and individual training and education sponsored by the center should be challenging. These events should place a productive amount of stress and adversity on individuals and subunits, with the intent of creating a shared sense of purpose and the necessity to cooperate in order to succeed. Under this fundamental principle, analytical training might include team projects that require multidisciplinary reports on complex issues given a short response time. Tabletop exercises might include: multiple scenario shifts requiring significant reallocation of resources; events that are linked to a tactical training exercise and that require communicating with units in the field; events that are no-notice, come-as-you-are; and events run on a 24/7 basis.

Leaders should also focus on making training and education opportunities relevant to the fusion center's mission. This requires leaders to analyze the center's mission statement, current and potential threats to public safety in the operating environment, and, given these factors, to determine what tasks the fusion center is likely to be called upon to perform. Having identified a task list, leaders can then prioritize those tasks, develop training and education strategies for each prioritized task, and allocate resources against these priorities.

The training and education plan should outline a formal orientation program for new detailees and employees. This will ensure that each member of the organization has a common understanding of the fundamental organizational goals, capabilities, and limitations. Additionally, fusion center leaders can use this as an opportunity to deliver instruction on systemic issues such as respecting privacy rights and ensuring operational security.

As with outside offers for funding, personnel, and equipment, fusion center leaders must ensure that outside offers to assist with training and education are consistent with the overall plan and needs of the center. Conducting training and education based on funding opportunities without relation to a prioritized task list that results from careful analysis is often counterproductive and can undermine morale. The operators who staff the fusion center know when training and education is relevant and realistic and tend to become disillusioned when these fundamentals are not achieved.

The list of considerations in developing a training and education plan includes:

Education

- Include a formal orientation program for new members
- Initial entry and continuing education on laws, regulations, and rules that govern the operations of the fusion center and the conduct of its members
- Initial entry and continuing education on fusion center mission, goals, objectives, functions, capabilities, and limitations
- Operating role and mission delineation between fusion center and partner agencies
- Composition, capabilities, and disposition of partner agencies
- Fusion center processes, products, and services to include instruction on how these items are requested, used, and disseminated
- Information-sharing policies and guidelines
- Facility, security, personnel, and information policies

Training

- Fusion center after action reviews of routine and crisis operations

- Tabletop and tactical training exercises
- Individual skill proficiency training and assessment (e.g., analyst training)
- Cross-training to ensure resiliency by having staff members minimally trained in second ary functions (e.g., WMD specialist assisting with natural-disaster response)
- Inculcation of new doctrinal concepts and statewide programs such as intelligence-led policing or operational initiatives focused on safeguarding citizens and property[22]

III. Operating the Fusion Center

Step 9: Develop Templates for Fusion Center Products and Services

Fusion center products and services are presented in numerous forms and venues. Examples of fusion center products include a comprehensive statewide intelligence assessment, a white paper assessing a particular threat to the state, a briefing to a member of the homeland security community outlining the response to a natural disaster, and tactical situational-awareness reports. With each fusion center product and service, the true measure of effectiveness is its ability to communicate relevant information to decision makers in a timely manner.

A fusion center's clients might include political leaders, members of public safety organizations, homeland security operators, other government agencies (federal, local, tribal, or regional partners), private-sector managers, and health-care managers. The hallmark of a professional fusion center is its ability to anticipate client needs and to incorporate feedback from clients into future products and services. This effort should take into consideration not only the content of fusion center products and services but also the format and method of dissemination.

For example, the fusion center should avoid bombarding key leaders with relatively insignificant information sent via e-mail. Daily reports designed for broad dissemination can also run the risk of becoming mundane and nonvalue-added for the intended audience. Similarly, some clients will desire oral briefings, while others will desire written products. A highly functioning fusion center will sort through these client preferences and deliver customized, user-friendly products and services tailored for the needs of the client.

The bottom-line measure of success is to translate this client knowledge into templated processes, products, and services so that routine and recurring situations can quickly be analyzed and reported. The routine delivery of products to fusion center customers should be viewed as imperative for a number of reasons:

- Well-functioning processes for routine and recurring situations can quickly be adapted for use with unusual or crisis situations; if ordinary reporting is broken, chances are that crisis reporting will be, too
- Allows for robust assessment of client needs and expectations
- Facilitates continuous improvement in anticipating client needs and meeting expectations
- Allows clients to provide further guidance, direction, and requests for additional information and analysis
- Helps fusion center leaders determine the frequency to which products and services should be provided
- Prompts the client to share relevant information with the center, thus improving the center's situational awareness and enhancing the information and analysis contained in future products

Typical products and services that fusion centers offer include:

- Daily intelligence and operations briefings to homeland security and law enforcement leaders that provide updates on threats and operational activities
- Products and briefings to support state executive and legislative branch homeland

security–related decisions
- Situational-awareness bulletins for broad dissemination that describe relevant incidents, issues of concerns, trends, indications of related activity, and requests for information[23]
- Routine briefings and products to critical infrastructure operators
- Quarterly and annual trend-assessment reports
- Ad hoc products and services in response to emerging or current events

Fusion centers must be more than information repositories. Context and analysis must be the focus of all center activities.

Step 10: Develop Information-Sharing Policies and Procedures

Information sharing is an all-inclusive imperative. It is a fundamental reason that fusion centers are being established around the country. It involves both internal fusion center information exchange and sharing among the fusion center's local, state, regional, federal, and private partners. Information sharing can occur in many forms, including text messages on situations of immediate tactical importance, multi-agency collaboration in criminal or terrorism investigations, in-depth white papers on systemic threats to public safety, public announcements, and routine conversations. Given the criticality of information sharing, developing fusion center policies and procedures that reward sharing is an absolute necessity.

The descriptions above were easy to develop. But where the rubber meets the road on information sharing, it is often an extreme challenge to respect and adhere to the regime that governs information protection, such as the federal classification rules, which are designed to protect information. While these rules permit sharing, the incentive structure associated with them punishes mistakes in releasing classified information without providing a countervailing incentive structure to reward sharing. The central organizing principle under this approach is to protect, compartmentalize, and control information. Fusion center leaders would do well to consider the underlying philosophy of the federal classification system when adopting information-sharing policies and procedures for their centers.

Many of these rules were developed to wage the Cold War struggle with Communism. A relatively small number of national leaders in the federal government managed this effort. Since few people needed to be "in the know," we placed a premium on information security. The resulting "classification levels are based on fear: the probability of information being disseminated to those that can cause serious damage to national security," according to the Congressional testimony of then-commander Mike Downing of the LAPD.[24]

This approach worked well in confronting Soviet communists in Western Europe—a very predictable adversary compared with present-day criminals and terrorists. These new legions can only be uncovered and neutralized by guardians who confront them having the highest possible level of situational awareness. This is what led Cathy Lanier, then–acting police chief of Washington, D.C., to "emphasize the importance of quickly sharing information—even if the information is not fully vetted" in her Congressional testimony.[25]

These law enforcement leaders have identified the central organizing principle for fusion center information-sharing policies and procedures: sharing information is usually more important than protecting it. To support the implementation of that principle, it is necessary to develop an incentive structure that rewards sharing enough to overcome the risk-averseness associated with information security rule regimes. Two strategies that will help create this incentive structure are peer evaluations and review boards.

Peer evaluations can be designed to evaluate partner agencies and individual detailees in their performance

as sharers. Many fusion centers incorporate peer evaluations on fusion center reports. These should be tracked, reviewed at governance board meetings, and used as an accountability mechanism. Fusion center leaders should know, for example, who is and who is not completing evaluations. These leaders must have visibility on the performance of partner agencies and individual detailees. This information can be used in a Compstat-like process to evaluate, solve problems, and hold partners accountable. It will also provide hard data on which individual performance can be evaluated.

Review boards should be designed to learn from honest mistakes rather than punish those who make mistakes.[26] If the central organizing principle is going to be information sharing, leaders will have to underwrite some mistakes when it comes to information protection. Assuming that information leaks are usually the result of honest mistakes or simple negligence, rather than purposeful acts of malfeasance, it is better to approach incidents with the intent to learn how the breakdown occurred and adopt practices to prevent future mistakes of a similar nature. Review boards can be adopted to make those determinations. The board's charter would be to learn from mistakes rather than punish those responsible. If such a board came across a case that might involve malfeasance, the board would refer that case to a separate investigative agency, such as an inspector general's office. Other helpful tips in building a state's information sharing environment include:

- Cataloging all information collectors, data providers, analyzers, and disseminators to identify the universe of those people and organizations that should be evaluated based on the quantity and quality of information that is shared
- Identification of collective (pertaining to more than one partner agency) or critical (may be collective or single-partner agency issue) information requirements and gaps to best focus intelligence and operations resources against the most pressing problems
- Mapping information-flow processes to identify crucial areas (e.g., incoming and outgoing avenues of information, multi-connected sharing points, and areas of vulnerability)
- Developing plans and notification protocols to communicate routine and crisis information to key leaders and partner agencies (including primary, secondary, and tertiary modes of communication)
- Training and education efforts on 28 CFR, part 23, which governs how data contained in federally funded intelligence systems are safeguarded and used[27]

Step 11: Create an Information Technology Architecture That Supports the Mission

In keeping with the theme of this document regarding financial constraints, the following information technology recommendations focus on policy issues. Given the complexity of state public safety operations, there is virtually a limitless supply of data that may have bearing on operational solutions.[28] Information technology enables people and organizations to sort quickly through those data. The reverse equation—people as enablers of technology—is not valid.

Leaders must guard against becoming too enamored with technological responses, while failing to consider human ability, organizational processes, and fundamental doctrines. While technology can simplify and speed up many tasks, it can also create confusion and bottlenecks when it is ill-suited for the available human operators and relevant organization or is not aligned with doctrinal approaches.

One classic example of a technological solution that did not align with organizational structure, mission, and culture is the FBI's Virtual Case File. Commissioned following the September 11 attacks, VCF was a computer program that was designed to help agents organize and share data related to terrorism. The FBI scrapped the program after investing hundreds of millions of dollars. VCF failed in its intended purpose because the effort to understand the FBI's organization, culture, and processes was not done up front. Instead, an attractive technology was selected first, and the FBI and the service provider went about trying to make VCF "fit" the Bureau. "Lawmakers and the contractor agreed that the intense pressure to get a product out to FBI agents following the terrorist attacks of September 11, 2001, contributed to the problem."[29]

Before reaching for technological answers, leaders must analyze the fusion center's mission requirements, evaluate the skills of its members, and articulate organizational capabilities. Technology can then be evaluated based on the likelihood that it will enhance mission accomplishment, be user-friendly, and be aligned with organizational capabilities and doctrinal approaches. Additionally, any new technology must be evaluated for how it will connect with the existing information technology infrastructure.

In assessing the need for the type of information technology that the fusion center may desire or make the best use of, the following end-state objectives should be considered:

- Development of a common database where all fusion center members can access:
  - o Catalog of fusion center members, their areas of responsibility (e.g., center director, shift leader, gang expertise, WMD specialist,meteorologist, virologist) and contact information
  - o Fusion center chain of command and organizational chart
  - o General information on ongoing and planned operations
  - o Calendar of events, training opportunities, etc.
  - o Administrative announcements
  - o Tracking system for internal and external support requests
- Posting of intelligence and operations briefings; the architecture should be configured to support the posting of briefings drafted at various security and sensitivity levels
- A repository for the vast majority of previously produced fusion center products (some products may be classified or otherwise operationally sensitive)
- Consistent with civil liberty protections and 28 CFR, part 23, searchable databases that contain information relating to the security of the state
- A method to allow external partners to access and provide information in relevant areas

Step 12: Adopt Fusion Center Security Measures

Safeguarding the physical infrastructure, operations, personnel, and information of the center is necessary to ensure uninterrupted and unimpeded delivery of products and services. Most fusion center locations, leadership names, and responsibilities are widely published and could be used for nefarious purposes. Additionally, natural disasters might affect fusion center performance. Should the fusion center's facilities, personnel, information, or operations be damaged or manipulated, the center's effectiveness would be seriously degraded. Avoiding or mitigating this result becomes particularly important in a crisis situation, when continuous and unencumbered performance is most valuable.

To avoid and mitigate such situations, fusion center leaders must implement appropriate security plans. Among the issues to consider when planning security for the fusion center are:

1. Physical Security

   - Site selection that factors in survivability and operability in a natural disaster and has appropriate separation from known potential hazards (e.g., chemical plants, power plants, commercial rail lines)
   - Fusion center unique identification cards
   - Key codes and entry locks
   - Guards and barriers
   - Traffic control patterns and checking personnel and vehicles desiring entry
   - Procedures that allow key personnel who do not routinely work at the center (e.g., governor, state police commander) access in a crisis
   - Lighting
   - Random security patrols
   - Establishment of a secondary site location

2. Operational

   - Balancing the need to share information with the need to protect operational security, sources, and methods will be an ongoing struggle in any interagency environment

- Operational security measures must be negotiated in MOAs and MOUs with partner agencies and addressed in written fusion center guidelines
- Sources and methods must be addressed
- Routine assessment of performance in completed cases; broad dissemination of lessons learned
- Assignment of responsibility to a specific person or sub-element to review practices and cases from other fusion centers; broad dissemination of lessons learned

3. Personnel

- Determine and prioritize fusion center positions that require a security clearance
- Ensure that individuals holding security clearances are aware of their responsibilities; require members to routinely validate such knowledge
- Train fusion center employees on the warning signs of individuals attempting to gain access to the facility or non-public information about the fusion center
- Establish a reporting mechanism for such activity
- Assist fusion center members to prepare their families for crisis situations
- Require members to validate family care plans to ensure that families are prepared to manage in a crisis without the member (who is needed—physically and mentally—in the fusion center); members must be prepared to operate with the knowledge that their families will not be in danger and are prepared to respond in emergency situations

4. Information

- Protect information infrastructure from unauthorized access
- Monitor systems for signs of unauthorized access; establish governance mechanisms to respond quickly
- Establish random checks of people leaving the facility[30]
- Provide initial entry and continuing education on applicable laws, regulations, and rules that govern information security and usage
- Establish oversight and inspection regimes to ensure that information is handled properly and purged when appropriate and that access to fusion center databases and resources is not abused
- Establish accountability mechanisms for individuals who violate established guidelines (See Step 10)
- Establish procedures for reviewing trends and taking appropriate actions to address systemic problems

> The true measure of fusion center effectiveness is its ability to provide timely and relevant information that influences policy development, decision makers, and operators in the field.

CONCLUSIONS

The recommendations and process-oriented steps contained in this document suggest a resource-independent method of enhancing fusion center operations. A fusion center can take many forms and perform numerous functions. Whether state leadership desires to have one organization dedicated to analyzing and managing response to all threats and hazards, or simply to focus on a limited array of issues and functions, the systemic issues to be addressed will remain the same. Though this paper is not exhaustive, the twelve suggested steps provide a fusion center, whether established or planned, with a road map for enhancing the state's ability to prevent—and, if necessary, to respond to—any type of threat.

1 The focus of this report is on state-led fusion centers. The authors acknowledge that some jurisdictions have established, or are in the process of establishing, major metropolitan area fusion centers. Whether the goal is to establish or refine the operations of a regional, state, or local fusion center, the recommendations contained here are intended to be applicable.

2 Remarks by Secretary of Homeland Security Michael Chertoff on September 11: Five Years Later, September 8, 2006.

3 For purposes of this report, operations centers are defined as those organizations that have as a primary mission the deployment, monitoring, and support of state and local assets responding to an incident—whether that incident is caused by natural or man-made events. Fusion centers, some of which include previously existing or newly established operations centers, involve the receipt, analysis, and dissemination of all-hazards information. It should be noted that numerous organizational terms have been used interchangeably to discuss the functions of today's fusion centers: "information clearinghouse," "operations center," "crisis center," "emergency management operations center," and various types of "command centers."

4 Consistent with the all-hazards approach of many fusion centers, the term "threat" indicates any natural or man-made occurrence that has the possibility of negatively affecting the citizenry, property, or government functions of a given jurisdiction.

5 "Information" is the overarching term used throughout this report to describe the various types of data and products that the fusion center may encounter. This includes intelligence (analyzed data) for the sake of linguistic simplicity. However, the reader should be cognizant of the difference between information and intelligence. Where it is important to the context of our writing, we have attempted to indicate whether we are referring to information or intelligence.

6 Todd Masse, Siobhan O'Neil, and John Rollins, "Fusion Centers: Issues and Options for Congress," Congressional Research Service, July 6, 2007.

7 See http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

8 It is important to recognize that state fusion centers are not the only entity that maintains contact with federal government law enforcement and homeland security agencies. State fusion centers often are managed by, or collaborate with, the governor's designated homeland security advisor, who has direct dealings with the federal government. In addition, other state and local entities that have responsibility for safeguarding numerous aspects of the jurisdiction may have routine contact with federal government authorities.

9 Information Sharing Environment Implementation Plan, Program Manager, Information Sharing Environment, November 2006, http://www.ise.gov/docs/ISE-impplan-200611.pdf.

10 Open for Business—Grants, Department of Homeland Security website, http://www.dhs.gov/xopnbiz/grants.

11 Fusion Center Guidelines, Law Enforcement Intelligence, Public Safety, and the Private Sector, http://it.ojp.gov/documents/fusion_center_guidelines.pdf.

12 Fusion Center Best Practices, A Massachusetts Perspective, Paul M. Connelly, Senior Homeland Security Advisor, Executive Office of Public Safety, http://www.nlectc.org/training/nij2006/connelly.ppt.

13 "Members" include "employees" who permanently staff the fusion center and "detailees" who are assigned to work in the fusion center by partner agencies. Fusion center members also include all internal and external personnel who work in or have routine interaction with the organization, such as contractors, consultants, and other professionals.

14 28 CFR, part 23 is a guideline for law enforcement agencies that operate federally funded multi-jurisdictional criminal intelligence systems; see http://www.cops.usdoj.gov/mime/open.pdf?Item=438.

15 Masse, O'Neil, and Rollins, "Fusion Centers."

16 The Joint Regional Intelligence Center (JRIC) in Los Angeles is funded mainly by its three sponsoring agencies: the FBI, the Los Angeles County Sheriff's Department, and the LAPD.

17 The Center for Policing Terrorism has provided consulting services for the last two years on a broad range of relevant issues to the ROIC, New Jersey's fusion center, and its sponsoring agency, the New Jersey State Police.

18 Masse, O'Neil, and Rollins, "Fusion Centers." See pages 29-31.

19 Those agencies that contribute financial resources that fund center operations or that provide other significant resources (e.g., a building, significant human resources) are the ones that typically control governance issues.

20 State and Local Fusion Centers, Department of Homeland Security, September 14, 2006, http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm; and Opening of Joint Regional Intelligence Center (JRIC), Los Angeles Police Department news release, July 25, 2006, http://www.lapdonline.org/newsroom/news_view/32984.

21 Speech to the 108th annual conference of the International Association of the Chiefs of Police, Toronto, Canada, ct. October 29, 2001.

22 Practical Guide to Intelligence Led Policing, New Jersey State Police, http://www.cpt-mi.org/pdf/NJPoliceGuide.pdf.

23 Multiple versions of these bulletins may be required, depending on the classification level, investigative sensitivity issues, and other types of information that may not be appropriate for disclosure to all audiences.

24 "Over-Classification and Pseudo-Classification: The Impact on Information Sharing," House Homeland Security Subcommittee on Intelligence, March 22, 2007.

25 Ibid.

26 The FAA uses such a system to investigate airline safety. The idea is to learn about mechanical, human, or other errors and to share that information as quickly as possible so that it can be used to improve overall airline safety. For more information, see http://www.faasafety.gov/about/mission.aspx.

27 See n. 14 above.

28 A successful fusion center becomes the repository of many types of seemingly unrelated data. Information may be provided by the general public or federal, state, local, private-sector, and academic partners. Fusion center leaders need to ensure that this information is appropriately safeguarded and available for use in assessing current and future threats and vulnerabilities to the state. The center's information technology architecture should account for the many security requirements and uses of the information flowing into and out of the organization.

29 Terry Frieden, "Report: FBI Wasted Millions on 'Virtual Case File,' " CNN.com, February 3, 2005. See http://www.cnn.com/2005/US/02/03/fbi.computers.

30 In a now-famous example, an employee of the Veterans Administration took a VA computer home to copy files onto a personal computer. A burglar stole the VA computer from the employee's home in what appeared to be a simple case of theft. See http://redtape.msnbc.com/2006/06/lost_va_data_wh.html.

Fellows

R. P. Eddy, *Senior Fellow*
Tim Connors, *Director*
Usha Sutliff, *Deputy Director*

The Manhattan Institute's Center for Policing Terrorism (CPT) connects a core group of police departments with some of the world's most prominent tactical and academic counter terrorism experts in order to provide local law enforcement with uniquely useful knowledge products, advice, insights and services. CPT incorporates what it learns from working closely with First Preventers into best practices manuals, and advocates for enhancing the capabilities of state, tribal, and local public safety agencies as a necessary component of our national security fabric.

The Manhattan Institute is a 501(C)(3) nonprofit organization. Contributions are tax-deductible to the fullest extent of the law. EIN #13-2912529