Fusion Center Guidelines

Developing and Sharing Information and Intelligence in a New World

Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level

Law Enforcement Intelligence Component

July 2005
Version 1

BJA Bureau of Justice Assistance

United States Department of Justice

The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security collaborated in the development of the fusion center guidelines contained in this report. Members of DOJ's Global Justice Information Sharing Initiative and the Homeland Security Advisory Council also supported this project, which involved numerous law enforcement experts and practitioners from local, state, tribal, and federal agencies, as well as public sector and private entities from across the country. The intent of the alliance was to provide a consistent, unified message and to provide a comprehensive guideline for developing a fusion center within a state or region.

The development of guidelines for fusion centers has been separated into three phases—law enforcement intelligence, public safety, and the private sector. Fusion center guidelines for the first phase—law enforcement intelligence—are complete. These guidelines may be used for homeland security efforts, as well as all crimes. This report includes an executive summary that includes an overview of the guidelines and their key elements. Also included in this report are additional resources, model policies, and tools for implementation. Guideline development for the second phase—public safety—is currently under way, with plans to incorporate the private sector phase.

The Role of Leadership

In developing our country's response to the threat of terrorism, public safety leaders from all disciplines have recognized the need to improve the sharing of information and intelligence across agency borders. Every law enforcement, public safety, and private sector official involved in information and intelligence sharing has a stake in this initiative. Leaders must move forward with a new paradigm on the exchange of information and intelligence.

Leaders are encouraged to embrace the guidelines set forth in this report and, when establishing a fusion center or participating in one, to ensure that these guidelines are followed. Information and intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center utilizes a common set of guidelines. The complete support of public safety leaders at all levels is critical to the successful implementation and operation of fusion centers.

Table of Contents

Executive Summary 1

Summary of Guidelines and Key Elements 5

Introduction—Fusion Concept and Functions 9

Fusion Center Guidelines Development 9
The Fusion Concept 10
Fusion Centers 14
Fusion Center Functions 16
State Strategy 17
Information Flow 18
A Phased Approach 19

Phase 1—Law Enforcement Intelligence Component 21

Methodology 21

Guidelines **25**

1. The NCISP and the Intelligence Process 25
2. Mission Statement and Goals 29
3. Governance 33
4. Collaboration 37
5. Memorandum of Understanding (MOU) 39
6. Database Resources 41
7. Interconnectivity 45
8. Privacy 49
9. Security 53
10. Facility, Location, and Physical Infrastructure 57
11. Human Resources 61
12. Training of Center Personnel 65
13. Multidisciplinary Awareness and Education 67
14. Intelligence Services and Products 69
15. Policies and Procedures 73
16. Center Performance Measurement and Evaluation 75
17. Funding 79

Next Steps 81

Appendix A: Focus Group Participants and Acknowledgements 83

Appendix B: Fusion Center CD Resources 87

Appendix C: HSAC Homeland Security Intelligence and Information Fusion Report (April 28, 2005) 93

Appendix D: Fusion Center Report Glossary 105

Appendix E: Acronyms 115

Executive Summary

The need to develop and share information and intelligence across all levels has significantly changed over the last few years. The long-standing barriers that built roadblocks among law enforcement agencies, public safety, and the private sector are slowly crumbling. Yet, the need to identify, prevent, monitor, and respond to terrorist and criminal activities remains a significant battle for the law enforcement, intelligence, and public safety communities.

The National Governors Association Center for Best Practices, January 2005 survey reveals that states ranked the development of state intelligence fusion centers as their second highest priority.

Through the support, expertise, and knowledge of law enforcement leaders from all components, the fusion center concept can become a reality. Each official has a stake in the development and exchange of information and intelligence and should act as an ambassador to support and further this initiative. It is the responsibility of leadership to implement and adhere to the fusion center guidelines.

The development and exchange of intelligence is not easy. Sharing this data not only requires strong leadership, it also requires the commitment, dedication, and trust of a diverse group of men and women who believe in the power of collaboration.

How can law enforcement, public safety, and private entities embrace a collaborative process to improve intelligence sharing and, ultimately, increase the ability to detect, prevent, and solve crimes while safeguarding our homeland? Recently, an initiative has emerged that incorporates the elements of an ideal information and intelligence sharing project—fusion centers ("center"). This initiative offers guidelines and tools to assist in the establishment and operation of fusion centers. The guidelines are a *milestone* in achieving a unified force among all levels of law enforcement agencies; public safety agencies, such as fire, health, and transportation; and the private sector. Fusion centers bring all the relevant parties together to maximize the ability to prevent and respond to terrorism and criminal acts. By embracing this concept, these entities will be able to effectively and efficiently safeguard our homeland and maximize anticrime efforts.

What Is the Fusion Center Guidelines Initiative?

As part of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC), in support of the Bureau of Justice Assistance, Office of Justice Programs, DOJ efforts to develop fusion center guidelines, recommended the creation of the Intelligence Fusion Center Focus Group.[1] Participants of the focus group included experts and practitioners from local, state, and federal law enforcement agencies as well as representatives from DOJ, the U.S. Department of Homeland

[1] Prior to integrating the public safety and private sector component into this initiative, the workgroup was referred to as the Fusion Center Intelligence Standards Focus Group.

Security (DHS), and the Federal Bureau of Investigation (FBI). In addition, members from national law enforcement organizations and currently operating fusion centers participated in the focus group's efforts. This focus group was tasked with recommending guidelines specifically for the law enforcement *intelligence* component of fusion centers.

In addition, the Homeland Security Advisory Council (HSAC or Council) Intelligence and Information Sharing Working Group has focused on prevention and information sharing by developing guidelines for local and state agencies in relation to the collection, analysis, and dissemination of terrorism-related intelligence in the context of fusion centers. The recommendations resulting from the DOJ initiative and HSAC's efforts lay the foundation for the development of fusion center guidelines for law enforcement intelligence, public safety, and private sector entities.

Through this landmark initiative, it is anticipated that these guidelines will be utilized to ensure fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities. These guidelines and related materials will provide assistance to centers as they prioritize and address threats posed in their specific jurisdictions for all crime types, including terrorism. In addition, these guidelines will help guide administrators in developing policies, managing resources, and evaluating services.

The development of guidelines for fusion centers has been separated into three phases—law enforcement intelligence, public safety, and the private sector. Fusion center guidelines for the first phase—law enforcement intelligence—are complete. These guidelines may be used for homeland security efforts, as well as all crimes. This report includes an executive summary that contains an overview of the guidelines and their key elements. Also included in this report are additional resources, model policies, and tools for implementation. Guideline development for the second phase—public safety—is currently under way, with plans to incorporate the private sector phase. Integrating these components will not be an easy task. It will take the hard work and dedication of many individuals.

Fusion:

Turning Information and Intelligence Into Actionable Knowledge

What Is the Fusion Process?

The concept of fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across levels and sectors of government. It goes beyond establishing an intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate and/or emerging threat-related circumstances and events. Data fusion blends data from different sources, including law enforcement, public safety, and the private sector, resulting in meaningful and actionable intelligence and information. The fusion process also allows for

relentless reevaluation of existing data in context with new data in order to provide constant updates. The fusion process turns information and intelligence into actionable knowledge.

What Is a Fusion Center?

A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (NCISP or Plan). The NCISP is regarded as the blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. The Plan contains over 25 recommendations that were vetted by law enforcement officials and experts from local, state, tribal, and federal agencies. The Plan embraces intelligence-led policing, community policing, and collaboration, and it serves as the foundation for the fusion center intelligence guidelines.

For the purposes of this initiative, **a fusion center is defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.** The intelligence component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity.

The principal role of the fusion center is to compile, blend, analyze, and disseminate 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 efforts to anticipate, identify, prevent, and/or monitor criminal activity.

The fusion process involves every level and sector (discipline) of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. For purposes of this report, the fusion process should be organized and coordinated on a statewide level, and each state should establish and maintain a center to facilitate the fusion process.

Although each fusion center will have unique characteristics, it is important for centers to operate under a consistent framework—similar to the construction of a building where each structure is unique, yet a consistent set of building codes and regulations are adhered to regardless of the size or shape of the building.

Why Should Fusion Centers Be Established?

The ultimate goal is to provide a mechanism where law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. As funds continue to be stretched to support numerous initiatives, it will be critical for government to accomplish ***more with less***. Fusion centers embody the core of collaboration, and as demands increase and resources decrease, fusion centers will become an effective tool to maximize available resources and build trusted relationships**.**

It is recommended that fusion centers adhere to these guidelines and integrate the key elements of each guideline to the fullest extent.

Summary of Guidelines and Key Elements

1. ***Adhere to the tenets contained in the National Criminal Intelligence Sharing Plan, and perform all steps of the intelligence process.***
   - ✓ Consult the tenets of the Plan, and utilize model standards and policies as a blueprint for establishing or enhancing the intelligence function within the center.

2. ***Collaboratively develop and embrace a mission statement, and identify goals for the fusion center.***
   - ✓ Develop the center's mission statement and goals collaboratively with participating entities.
   - ✓ Identify customer needs, define tasks, and prioritize functions.
   - ✓ Ensure the mission statement is clear and concise and conveys the purpose, priority, and role of the center.
   - ✓ Include the name and type of the center, what the center does, and whom the center serves in the mission statement.

3. ***Create a representative governance structure.***
   - ✓ Ensure all participating agencies have a voice in the establishment and operation of the fusion center.
   - ✓ Ensure participating entities are adequately represented within the governance structure.
   - ✓ Compose the governing body with officials who have authority to commit resources and make decisions.

4. ***Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies.***
   - ✓ Maintain a diverse membership to include representatives from local, state, tribal, and federal law enforcement.
   - ✓ Conduct regular meetings with center personnel, and participate in networking groups and organizations.
   - ✓ Educate and liaise with elected officials and community leadership to promote awareness of center operations.
   - ✓ Integrate public and private sector entities into the intelligence function, as appropriate.

5. ***Utilize MOUs or other types of agency agreements, as appropriate.***
   - ✓ Educate and consult legal advisors early in the fusion center development process.
   - ✓ Use an MOU to lay the foundation for a collaborative initiative, founded on trust, with the intent to share and exchange information.
   - ✓ At a minimum, consider including the following elements in fusion center MOUs:

     - Involved parties
     - Mission
     - Governance
     - Authority
     - Security
     - Assignment of personnel (removal/rotation)
     - Funding/costs
     - Civil liability/indemnification issues
     - Policies and Procedures
     - Privacy
     - Terms
     - Integrity control
     - Dispute resolution process
     - Points of contact
     - Effective date/duration/ modification/termination
     - Services
     - Deconfliction procedure
     - Code of conduct for contractors
     - Special conditions
     - Protocols for communication and information exchange

6. ***Leverage the databases and systems available via participating entities to maximize information sharing.***
   - ✓ Obtain access to an array of databases and systems. At a minimum, consider obtaining access to driver's license information, motor vehicle registration data, location information, law enforcement and criminal justice systems or networks, and correctional data.
   - ✓ Become a member of a regional or state secure law enforcement network, such as the Regional Information Sharing Systems® (RISS)/Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) system, the Homeland Security Information Network (HSIN), or the FBI's Law Enforcement Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx).

7. ***Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development and allow for future connectivity to other local, state, tribal, and federal systems. Use the Global Justice Extensible Markup Language (XML) standard for future database and network development.***
   - ✓ Establish formal communications protocols, and ensure effective and efficient information exchange.
   - ✓ Develop and implement a communications plan, and ensure secure and redundant communications.
   - ✓ Ensure communications and systems access policies including consequences for noncompliance.
   - ✓ Consider utilizing the Organization for the Advancement of Structured Information Standards (OASIS)-ratified Common Alerting Protocol (CAP) to enable the exchange of emergency alert and public warning information over data networks and computer-controlled warning systems.

8. ***Develop, publish, and adhere to a privacy and civil liberties policy.***
   - ✓ Develop, display, adhere to, and train personnel on the center's privacy policy.
   - ✓ Consult the Fair Information Practices when developing a privacy policy.
   - ✓ Incorporate applicable local, state, and federal privacy laws into the center's privacy policy.
   - ✓ Ensure all other policies and internal controls are consistent with the center's privacy policy.
   - ✓ Establish a process for tracking and handling privacy complaints or concerns.

9. ***Ensure appropriate security measures are in place for the facility, data, and personnel.***
   - ✓ Develop, publish, and adhere to a security plan, and ensure proper safeguards are in place.
   - ✓ Ensure security plans are marked, handled, and controlled as sensitive but unclassified (SBU) information.
   - ✓ Obtain appropriate security clearances for personnel within the center and key decision makers who need access.
   - ✓ Conduct background checks on personnel.
   - ✓ Train personnel on the center's security protocols.
   - ✓ Consult Global's *Applying Security Practices* document and resource materials when developing a security plan.

10. ***Integrate technology, systems, and people.***
    - ✓ Colocate personnel and/or utilize virtual integration to bring technology, systems, and people together.
    - ✓ Base the selection of a site on the functional needs of the center.
    - ✓ Plan, identify, design, train, implement, and adhere to a physical security plan and a contingency plan.

11. *Achieve a diversified representation of personnel based on the needs and functions of the center.*

- ✓ Maintain a 24-hour-a-day/7-day-a-week operation when feasible.
- ✓ Require a minimum term commitment for full-time center personnel.
- ✓ Adhere to the *Law Enforcement Analytic Standards* booklet and other relevant analytic publications available through the International Association of Law Enforcement Intelligence Analysts (IALEIA) when hiring personnel to perform the analytic function.

12. *Ensure personnel are properly trained.*

- ✓ Adhere to the training objectives outlined in the *National Criminal Intelligence Sharing Plan*.
- ✓ Ensure center personnel meet the minimum training standards outlined in the report "Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies."
- ✓ Ensure center personnel receive training on facility and information security, operations, policies, and procedures.

13. *Provide a multitiered awareness and educational program to implement intelligence-led policing and the development and sharing of information.*

- ✓ Ensure appropriate noncenter personnel involved in the intelligence process are aware of the center's functions.
- ✓ Develop and disseminate outreach and educational materials to officers, analysts, policymakers, and others.

14. *Offer a variety of intelligence services and products to customers.*

- ✓ Produce strategic and tactical products to support the mission and priorities of the center.
- ✓ Consult the *Law Enforcement Analytic Standards* booklet to ensure development of professional quality analytic products.

15. *Develop, publish, and adhere to a policies and procedures manual.*

- ✓ Use a standardized format to allow for easy reading, filing, retrieving, and correcting.
- ✓ Implement an annual review of center directives, and purge or revise outdated policies and procedures.
- ✓ Ensure personnel have access to the latest policies and procedures manual.

16. *Define expectations, measure performance, and determine effectiveness.*

- ✓ Design performance measures based on the center's core mission, goals, and objectives.
- ✓ Ensure performance measures are valid, reliable, measurable, and quantifiable.
- ✓ Develop an evaluation process to gauge the adequacy, appropriateness, and success of center services.
- ✓ Use performance measures and an evaluation process to make decisions and allocate resources.
- ✓ Utilize performance measures to track progress and ensure accountability.
- ✓ Inform center personnel of performance and progress on a regular basis.

17. *Establish and maintain the center based on funding availability and sustainability.*

- ✓ Identify center needs and available funding sources, to include local, state, federal, and nongovernmental sources.
- ✓ Establish an operational budget and adhere to reporting requirements.

A companion CD has been developed in conjunction with the "Fusion Center Guidelines" report. This CD will contain sample policies, checklists, resource documents, and links to Web sites that are referenced throughout the "Fusion Center Guidelines" report. The fusion center resources are also available at the Global Web site: http://it.ojp.gov.

This Page Is Left Blank Intentionally

Introduction—Fusion Concept and Functions

As criminal and terrorist activity continue to hinder the safety of our nation's citizens and visitors, the ability to quickly exchange relevant information and intelligence becomes increasingly critical. Over the last few years, significant progress has been made in breaking down barriers and improving information exchange. Policymakers and leaders have recognized the importance of creating an environment where intelligence can be securely shared among law enforcement, public safety agencies, and the private sector. Although strides have been made, there is still much work ahead. There is still an urgent need to rigorously refine and accommodate our rapidly changing world.

Many obstacles have been encountered that have impacted the ability to share intelligence, such as the lack of trusted partnerships; disparate, incompatible, and/or antiquated communications computer systems and software; the need to query multiple databases or systems; the lack of communication; the lack of standards and policies; and legal and cultural issues.

These barriers have proved to be difficult hurdles. Yet, there are steps that can be taken to overcome these issues and create a proactive environment for the successful exchange of intelligence.

Information systems contribute to every aspect of homeland security. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Databases used for federal law enforcement, immigration, intelligence, public health, surveillance, and emergency management have not been connected in a way that allows us to comprehend where information gaps and redundancies exist.

We must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

The National Strategy for Homeland Security
July 2002

Fusion Center Guidelines Development

Multiple entities have been working diligently to resolve the issues that have hindered our criminal justice community. Through DOJ, members of Global have developed recommended guidelines to enhance justice information sharing.[2] Some examples include the *National Criminal Intelligence Sharing Plan* (NCISP or Plan), the *Privacy Information Quality Policy Development for the Justice Decision Maker*, the *Applying Security Practices to Justice Information Sharing*, and the Global Extensible Markup Language (XML) Data Model (Global JXDM). DOJ's Global represents over 30 law enforcement organizations throughout the country, at all levels of government.

Through the Global Intelligence Working Group (GIWG) (one of the four working groups of Global), intelligence issues, concerns, and obstacles have been addressed. Most recently, the CICC,[3] supported the development of the Intelligence Fusion Center Focus Group. This group was tasked with recommending guidelines specifically for the law enforcement intelligence component of fusion

[2] For more information regarding Global, visit www.it.ojp.gov.
[3] The CICC was established as a result of recommendations contained in the NCISP. The CICC is composed of local, state, and federal entities and advises the U.S. Attorney General on matters relating to criminal intelligence.

centers. The focus group was also tasked with recommending related model policies and procedures to support this initiative. The focus group members recognized the need and importance of integrating all public safety and private partners.

In addition, presidential directives have been promulgated that provide guidance to local and state entities regarding prevention and response to criminal and terrorist activities.[4] In furtherance of these directives, the HSAC Intelligence and Information Sharing Working Group, which focuses on prevention and information sharing, has been developing guidelines for local and state agencies in relation to the collection, analysis, and dissemination of terrorism-related intelligence in the context of fusion centers. The Council provides advice and recommendations to the U.S. Department of Homeland Security (DHS) Secretary on matters related to homeland security. The Council is comprised of leaders from state and local governments, first responder communities, the private sector, and academia.[5] The recommendations and findings resulting from the HSAC's Intelligence and Information Sharing Working Group efforts support the development of fusion center guidelines for public safety and private entities (Appendix B).

It is clear that all levels of government, the private sector, and nongovernmental organizations must work together to prepare for, prevent, respond to, and recover from terrorist and criminal events. Through the hard work, dedication, and commitment of the individuals participating in the efforts summarized above, the appropriate guidelines, tools, and information will be available to all entities involved. In addition, a collaborative environment will result in a consistent, unified approach to prevention and response.

The Fusion Concept

Law enforcement has always been aware of the key role that information and intelligence play in prevention and response. Although it is impossible to protect every potential target from every conceivable method of attack, there are a number of strategies that can be implemented to maximize this ability. In addition, further refinement in the intelligence and information sharing arena will maximize the ability to respond quickly and efficiently if an incident occurs.

Effective terrorism-related intelligence information and crime prevention, protection, preparedness, and response depend on timely and accurate information about the enemy, their operations, their support mechanisms and structure, their targets, and their attack methods. This

[4] Homeland Security Presidential Directive 8 (HSPD-8) was issued with the purpose of establishing policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities of federal, state, and local entities. HSPD-5 addresses the management of domestic incidents and identifies steps for improved coordination in response to incidents. It requires DHS to coordinate with other federal departments and state, local, and tribal governments to establish a National Response Plan (NRP) and a National Incident Management System (NIMS). Each of these items plays a role in the establishment of fusion centers and lays a foundation for enhanced information and intelligence sharing among all levels of law enforcement, public safety, and the private sector. For more information regarding HSPD-8, HSPD-5, NRP, and NIMS, visit www.ojp.usdoj.gov/odp/assessments/hspd8.htm.

[5] More information on HSAC can be accessed at www.dhs.gov/dhspublic/display?theme=9&content=3386.

information should serve as a guide for efforts to rapidly identify both immediate and long-term threats; identify persons involved in terrorism-related and criminal activities; and guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

This concept, however, represents a paradigm shift from a responsive approach to a preventive approach. Historically, law enforcement and public safety have tended to react to events rather than proactively prevent and detect events. However, since September 11, 2001, it was determined that both approaches are critical to an overall strategy to secure our homeland and decrease criminal activities. September 11, 2001, also confirmed how critical local, state, tribal, and federal law enforcement agencies are in collecting important information and intelligence ultimately impacting the nation's overall ability to prevent terrorism-related and criminal activities. Over 18,000 local, state, and tribal communities representing over 800,000 law enforcement officers are the front lines that support these efforts. Coupled with data from nontraditional intelligence collectors (e.g., fire, transportation), data fusion represents a mechanism that can dramatically improve information and intelligence sharing.

As a result of the need to amalgamate diverse data from various sources, the concept of fusion emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. On the surface, it would appear that defining fusion would be a difficult task. Although the concept of fusion is new to the law enforcement community, fusion is not new to many other industries. In fact, fusion has been discussed and/or utilized in the transportation and aviation industry, satellite imaging, meteorology and weather forecasting, sensory imaging, and military and defense activities.

As a result, a number of definitions have surfaced over the years, and many groups have attempted to fine-tune and enhance the definition of fusion. One of the most well-known references to data fusion comes from the U.S. Department of Defense (DoD). DoD defined data fusion as a *multilevel, multifaceted process dealing with the automatic detection, association, correlation, estimation, and combination of data and information from single or multiple sources*. The DoD model is based on a hierarchical four-phase approach, including object refinement, situation refinement, threat refinement, and process refinement.[6] Some researchers believe this definition is too general and have attempted to enhance the definition of data fusion. For example, Dr. Lucien Ward, Professor at Ecole des Mines (Paris), defines data fusion as a *formal framework used to express the convergence of data from different sources in which is expressed the means and tools for the alliance of data that originated from different sources*.[7]

---

[6] U.S. Department of Defense, "Data Fusion Lexicon," Data Fusion Subpanel of the Joint Directors of Laboratories, Technical Panel for C3, 1991.

[7] L. Wald, A European proposal for terms of reference in data fusion, *International Archives of Photogrammetry and Remote Sensing*, Vol. XXXII, Part 7, pp. 651-654, 1998.

Others, however, have defined it further by explaining that the data fusion process is characterized by its ability to combine possibly uncertain, incomplete, and contradictory data, perhaps resulting in data or information of improved quality. The fusion (or merger) process can also abstract data resulting in a reduced, more specific, amount of data.[8]

Desforges and Starr, authors of "Strategies in data fusion – sorting through the tool box," define data fusion as *a process that combines data and knowledge from different sources with the aim of maximizing the useful information content, for improved reliability or discriminate capability, while minimizing the quantity of data ultimately retained.*[9]

For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across levels and sectors of government. It goes beyond establishing an intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate and/or emerging, threat-related circumstances and events. Data fusion blends data from different sources including law enforcement, public safety, and the private sector, resulting in meaningful and actionable intelligence and information. The fusion process turns information and intelligence into knowledge. The primary emphasis of fusion is to identify emerging terrorism-related threats and risks as well as to support ongoing efforts to address criminal activities. It is anticipated that the fusion process will:

Fusion:

Turning Information and Intelligence Into Actionable Knowledge

- Allow local and state entities to better forecast and identify emerging crime, public health, and quality of life trends.
- Support multidisciplinary, proactive, risk-based, and community-focused problem solving activities.
- Provide a continuous flow of information and intelligence to officials to assist in developing a depiction of evolving threats.
- Improve the delivery of emergency and nonemergency services.

A formal data fusion framework represents and provides tools to manage different information. Data fusion can result from statistical analysis, mathematical models, and/or algorithms. The approach to use depends on different aspects, such as the type of data, the requirements of the applicant, and the reliability desired.[10]

---

[8] Ronnie Johansson, *Information Acquisition in Data Fusion Systems*, November 2003.

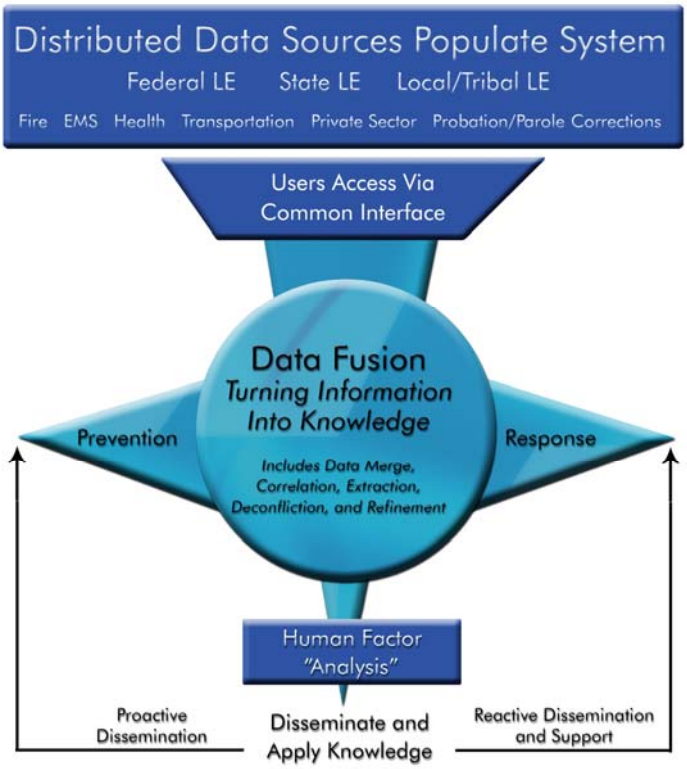
[9] M. Desforges, and A. Starr, "Strategies in data fusion – sorting through the tool box," In Proceedings, *EuroFusion98 International Conference on Data Fusion* (editors Bedworth and O'Brien), 1998, pp. 85-90.

[10] Hervaldo S. Carvalho, Claudionor J. N. Coelho, Wendi B. Heinzelman, and Amy L. Murphy, "A General Data Fusion Architecture," 2003.

Moving from a functional model to a working implementation in a real environment involves a number of design considerations, including what information sources to use, what fusion architecture to employ, and communication protocols.[11] For purposes of this initiative, the following steps are offered as a foundation to illustrate the fusion process: data input, data merging, correlation and association, data extraction, deconfliction, data refinement based on system results/user query, human analysis, and dissemination.[12] Information and intelligence should be validated as to credibility and reliability. Center personnel will utilize fused and analyzed information to provide value-added intelligence products that support the development of performance-driven, risk-based prevention, response, and consequence management programs.

To illustrate the fusion process within a conceptualized fusion center concept, Figure 1 depicts a distributed capability, populated by multiple and diverse data sources. Data is blended or "fused." Users access the data via a common interface, extracting, analyzing, and disseminating information based on need and current demands. Although it is anticipated that fusion and fusion centers will primarily be used for preventive and proactive measures, the process will also be critical if an incident occurs, providing information to responders as well as officials, media, and citizens.

Figure 1 – Fusion Process



[11] Ronnie Johansson, *Information Acquisition in Data Fusion Systems,* November 2003.

[12] It is important to note that these steps are a result of combined sources as well as specific needs for information and intelligence fusion centers. It is the intent of these technological steps to correspond to the intelligence cycle.

Criminal and terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism-related information. It can come through the efforts of the intelligence community; local, state, tribal, and federal law enforcement authorities; other government agencies (e.g., transportation, healthcare); the general public; and the private sector. In order to implement an effective fusion process, a number of issues must be addressed, including the following:

- The use of common terminology, definitions, and lexicon by all stakeholders.
- Up-to-date awareness and understanding of the global threat environment.
- A clear understanding of the linkages between terrorism-related and nonterrorism-related information and intelligence.
- Clearly defined intelligence and information requirements that prioritize and guide planning, collection, analysis, and dissemination efforts.
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process.
- Understanding and elimination of impediments to information collection and sharing.
- Extensive and continuous interaction with the private sector and with the public at large.
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories.
- Extensive participation of subject-matter experts in the analytical process.
- Capacity to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

It is anticipated that through the use of fusion centers and by integrating guidelines, model templates, policies, and tools, the outstanding issues hindering our nation's ability to seamlessly develop and share information and intelligence will be minimized.

Fusion Centers

The ability to coordinate effective responses in the event of a terrorist attack is one of the most challenging priorities facing our nation. It is imperative that all appropriate means to combat terrorism, respond to terrorist attacks, and reduce criminal activity are employed. This section will define fusion centers; summarize the basic functions of a fusion center; and provide a summary comparison of fusion centers, intelligence centers, and emergency operations centers. For purposes of this report, fusion center is defined as follows:

> **A fusion center is a collaborative effort of two of more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, investigate, apprehend, and respond to criminal and terrorist activity.**
>
> **Components of a fusion center include the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Other components include public safety, homeland security, private sector, and critical infrastructure.**

Fusion centers are not traditional intelligence centers nor do they perform the same functions as emergency operations centers. It is important to note that although these centers are different and have unique missions, they must also work together and understand each others' goals and priorities. If an incident occurs, all these resources will be needed to successfully minimize loss and apprehend suspects. Fusion centers are threat-driven and act as an effective framework for prevention, while intelligence centers are specific to investigative case support. Emergency Operations Centers focus on disaster recovery efforts (both natural and man-made).

Important intelligence that may forewarn of a future attack may be derived from information collected by local, state, tribal, and federal law enforcement agencies; public safety agencies; and private sector entities through crime control and other normal activities, as well as by people living and working in our communities.

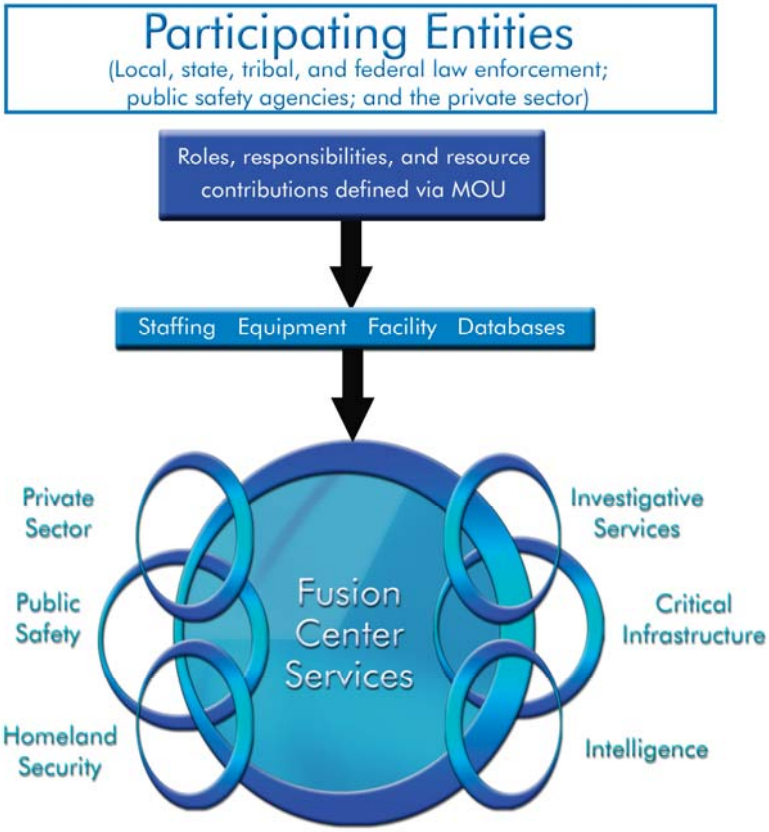
Fusion centers embody the core of collaboration. The goal of collaboration is to increase capacity, communication, and continuity of service while decreasing duplication.[13] As demands increase and resources decrease, collaboration becomes an effective tool to maximize resources and build trusted relationships**. In a recent survey conducted by the National Governors Association (NGA) Center for Best Practices, responding states ranked the development of a state intelligence fusion center as their second highest priority.**[14] This is significant and indicates a need to quickly provide information, materials, and guidelines to assist in establishing and operating fusion centers.

In an attempt to visualize the components of a fusion center, Figure 2 is offered as an example. As illustrated, the fusion center concept embraces the collaboration of numerous resources, maximizing and streamlining operations, while moving jointly toward a common goal. The example depicts participating entities using memorandums of understanding (MOU) to define their roles, responsibilities, and contributions toward the center. These resources funnel into a central location, the fusion center. Here, authorized personnel use the resources and information to assist investigative services, intelligence services, homeland security, and public safety operations and integrate critical infrastructure functions and private partnerships. Participants are subject to all the policies and procedures that guide center operations. Appropriate information and intelligence is then disseminated to authorized recipients and used to proactively investigate crimes and threats.

[13] C. R. Pete Petersen, M.Ed., *Community Collaboration*, March 4, 2003.

[14] NGA Center for Best Practices, *Homeland Security in the States: Much Progress, More Work,* January 24, 2005.

Figure 2 – Fusion Center Components



It is anticipated that fusion centers will act as an analytical hub, processing, evaluating, and disseminating critical information for law enforcement, public safety, and private partners. Fusion centers will focus on the analysis and collaboration process and will become a repository for the amalgamated information that flows through the center. Ultimately, fusion centers will become the nerve center for investigative support, intelligence sharing, homeland security and public safety, and private sector partners.

Fusion Center Functions

The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorism intelligence and other information (including but not limited to threat, public safety, law enforcement, public health, social service, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal activity. This criminal intelligence should be both strategic (i.e., designed to provide general guidance of patterns and trends) and tactical (i.e., focused on a specific criminal event). To be meaningful, the fusion center must do more than a one-time collection of law enforcement information. It must include developing the capability to "blend" on an ongoing basis—law enforcement information with other important information, such as public health, transportation, financial services, and social services, in order to rapidly identify emerging threats; support multidisciplinary, proactive, and community-focused problem-solving activities;

support predictive analysis capabilities; and improve the delivery of emergency and nonemergency services.

One of the principal outcomes should be the identification of terrorism-related leads—in other words, any "nexus" between crime-related and other information collected by local, state, and private entities and a terrorist organization and/or attack. The fusion process does not replace or replicate mission-specific intelligence and information management processes and systems. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may be reflective of an emerging threat condition. Some of the recommended goals and functions for fusion centers include the following:

- Serve as a receipt-and-dissemination hub for law enforcement information provided by federal entities, such as that provided by the FBI's Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx) and the Homeland Security Information Network (HSIN).
- Serve as the initial point of contact for the public and private sector personnel to report suspicious circumstances or threat-related information.
- Serve as the primary point of contact to report criminal/terrorist information to the local Joint Terrorism Task Force (JTTF) and DHS Homeland Security Operations Center (HSOC).
- Include the capability of blending law enforcement information and intelligence.
- Collect, analyze, and disseminate "all-crimes" information, so as to identify emerging patterns and trends. Evaluate and reevaluate the process, new data, and emerging threats.
- Adopt and adhere to a statewide strategy to examine the information exchanges of the states law enforcement and homeland security partners, including dissemination of information by the state Homeland Security Advisor to law enforcement.
- Maintain an up-to-date statewide risk assessment.

Each of these areas can be expanded to include a number of critical tasks and responsibilities. In order to successfully achieve these goals, it is important that the first responder and private community, along with the public, are a part of the fusion center concept. Integrating nontraditional consumers of information and intelligence is a key component.

The responsibilities of fusion centers are immense. It is essential that guidelines as well as sample policies and templates be developed to assist in establishing and operating fusion centers.

State Strategy

The fusion process involves every level and sector (discipline) of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process due to the relationship between crime and terrorism and due to the fact that in many cases, law enforcement authorities are best suited to coordinate statewide and local

fusion efforts. As part of the HSAC Working Group recommendation, it was proposed that fusion centers be established in every state. The fusion process should be organized and coordinated on a statewide level, and each state should establish and maintain an analytic center to facilitate the fusion process. Furthermore, each state fusion center should regularly collaborate and coordinate with other fusion centers across state lines. This effort will further enhance criminal/terrorism information and intelligence sharing among law enforcement, public safety, and private entities.

The functions within a state fusion center should be based on a process that incorporates the intelligence cycle, including requirements, priorities, identified collectors, indicators for the collectors to be aware of, collection mechanisms, methods of analysis, and production and dissemination of reports and assessments to the appropriate recipients. The first responder and private sector, along with the public, are a critical part of this plan in that they need to be brought into the intelligence cycle by being the collectors of this information based on requirements.

Each major urban area may want to establish a similar capacity ensuring that it is interlinked with the state center. Other localities, tribal governments, and even the private sector should develop a process to interlink to these state fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activity or circumstances.

Efforts should be organized and managed on a geographic basis and scalable so adjustments can be made based on changes in the operating and/or threat environment. And, while national guidelines should guide the institutionalization of the process, the actual technological infrastructure and operational protocols used by individual jurisdictions should be based on the management structure, specific needs, and capabilities of each individual jurisdiction.

Information Flow

With fusion centers being established around the country, it is important to have a clear understanding of how information flows both vertically and horizontally among all state, local, tribal, and federal government agencies and private entities, as well as who should receive information and who should disseminate information. Successful counterterrorism efforts require that local, state, tribal, and federal law enforcement agencies along with public safety and private sector entities have an effective information sharing and collaboration capability, to ensure they can seamlessly collect, blend, analyze, disseminate, and use information and intelligence regarding threats, vulnerability, and consequences in support of prevention, response, and consequence-management efforts.

Intelligence and information should be provided based on the needs of the user. Although fusion center participants may include emergency management, public health, transportation, public works, and the private sector, each discipline may not need the same level of detail (i.e., fire officials and emergency management officials may not need specific suspect information that law enforcement requires depending upon the issues and/or incident). Fusion centers should exchange information with

appropriate federal partners such as DOJ (e.g., FBI, JTTFs, U.S. Marshals), DHS (e.g., Customs and Border Protection), High Intensity Drug Trafficking Areas (HIDTA), RISS centers, and other information sharing initiatives.

One of the roles of the fusion center is to serve as a conduit to provide relevant intelligence to appropriate local, state, regional, tribal, and federal public and private officials to support prevention and response efforts. In order to effectively and efficiently determine the information flow among these entities, it is recommended that the Justice Information Exchange Model (JIEM) be employed. The JIEM was created by SEARCH, The National Consortium for Justice Information and Statistics, and supported by the Bureau of Justice Assistance. The JIEM is a conceptual framework that presents the flow of information between agencies; defines the key events that trigger the need to share information; identifies the agencies involved in the exchange; and describes the nature of the information exchange, irrespective of whether one is analyzing a justice or nonjustice system exchange.

A Phased Approach

The development of guidelines for fusion centers has been separated into three phases—law enforcement intelligence, public safety, and the private sector. Guidelines for the first phase—law enforcement intelligence—are complete and are included in this report. Guideline development for the second phase—public safety—is currently under way, with plans to integrate the private sector phase. Each phase will include a summary of the methodology used to develop guidelines, a summary of the guidelines, and a detailed section focused on each individual guideline.

By integrating these guidelines, many of the obstacles discussed earlier can be resolved. In addition, guidelines can help guide administrators in developing policies, managing resources, and evaluating services. Integrating all of these components will not be an easy task. It will take the hard work and dedication of many individuals.

The ultimate goal is to provide a mechanism where law enforcement, public safety, and private partners can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. A police officer, fireman, or building inspector should not have to search for bits of information. They should know to call one particular place—the state fusion center.

The recommendations contained in the report represent the key components and issues to consider when establishing fusion centers.

This Page Is Left Blank Intentionally

Phase I—Law Enforcement Intelligence Component

Methodology

Early in 2002, the International Association of Chiefs of Police (IACP) convened a Criminal Intelligence Sharing Summit attended by law enforcement executives and intelligence experts from across the country. Participants agreed that all law enforcement agencies must work together toward a common goal: developing the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies.

> ***". . . we must create new ways to share information and intelligence both vertically, between governments, and horizontally, across agencies and jurisdictions . . . efforts with the Global Intelligence Working Group to create a National Criminal Intelligence Sharing Plan . . . is a helpful and welcome response."***
>
> ***—Former Homeland Security Secretary Tom Ridge***
> ***October 23, 2003, Philadelphia, PA***

The Summit led to the creation of the Global Intelligence Working Group (GIWG). The GIWG, one of four working groups under Global,[15] was tasked with recommending a national intelligence plan. Members of the GIWG include representatives from law enforcement and justice organizations at all levels of government.

The GIWG promoted intelligence-led policing, recommended leveraging existing systems, and addressed the current and future needs of law enforcement agencies. For purposes of this report, intelligence is defined as the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature. Intelligence-led policing is the collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels.[16]

> ***"The Plan represents law enforcement's commitment to take it upon itself to ensure that we do everything possible to connect the dots, whether it be a set of criminal dots or a set of terrorist dots."***
>
> ***—Former U.S. Attorney General John Ashcroft***
> ***May 14, 2004, Washington, DC***

The GIWG proposed 28 recommendations and action items for implementation, which are outlined in the *National Criminal Intelligence Sharing Plan* (NCISP or "Plan").[17] An event was held at the DOJ Great Hall of Justice on May 14, 2004, to publicly support the recommendations and the Plan. Officials from local, state, and federal law enforcement agencies were present. It is important to note that several million dollars was included in the President's 2006 budget for implementation of the Plan. The recommendations contained in the Plan pertain to a wide spectrum of intelligence issues and concerns, including:

---

[15] For more information regarding Global, visit www.it.ojp.gov.
[16] *National Criminal Intelligence Sharing Plan*. Appendix A. October 2003.
[17] A copy of the *National Criminal Intelligence Sharing Plan* can be obtained at http://it.ojp.gov/topic.jsp?topic_id=93.

- Standards for management.
- Criminal Intelligence Coordinating Council.
- Institutionalism and outreach.
- Protection of rights and privacy.
- Standards for process.
- Better sharing of classified information.
- Standards for training.
- Connectivity.

As mentioned in the introduction, as part of Global, the CICC,[18] in support of DOJ's efforts to develop fusion center guidelines, recommended the creation of the Fusion Center Intelligence Standards Focus Group, to further many of the tenets outlined in the Plan.

On August 24 and 25, 2004, the focus group met in Atlanta, Georgia. Mr. Peter Modafferi, Chief of Detectives at the Rockland County, New York, District Attorney's Office, chaired the focus group. The focus group consisted of a variety of local, state, and federal law enforcement agencies from across the country. The focus group participants brought experience and expertise to the process. Some members have been involved with developing centers within their regions and offered example policies and materials to assist in this initiative.

During the first meeting of the focus group, Chief Modafferi explained the importance of intelligence, intelligence-led policing, and information sharing. During his presentation, he mentioned the need to establish an information and intelligence sharing environment that creates a generation of police officers who understand the value of intelligence and how information becomes intelligence. Throughout the meeting and subsequent communications, participants were encouraged to discuss and share best practices resulting from the establishment and operation of their centers or initiatives. The materials contained in this portion of the report represent the hard work from these individuals. The focus group met again on January 12-13, 2005, in Washington, DC, to finalize the recommendations and endorse the model policies and templates. These guidelines are the foundation for the intelligence component of fusion centers and takes intelligence sharing to the next level.

The focus group members recommended that the intelligence component include all crime types and that centers provide an array of intelligence services. In addition, the group recommended that centers be scalable based on the needs of the city, state, or region and should conduct tactical, operational, and strategic intelligence functions in support of criminal investigations.

[18] The Criminal Intelligence Coordinating Council (CICC) was established as a result of recommendations contained in the NCISP. The CICC is composed of local, state, and federal entities and advises the U.S. Attorney General on matters relating to criminal intelligence.

As a result of the focus group's work, 17 fusion center law enforcement intelligence guidelines were developed. In addition, the focus group developed sample policies and tools as well as a Resource CD to assist agencies in integrating the guidelines. These guidelines were presented to and supported by the CICC, the GIWG, the Global Advisory Committee, and DOJ's Justice Intelligence Coordinating Council (JICC). These guidelines were also approved by each component of the U.S. Department of Homeland Security.

This Page Is Left Blank Intentionally

The NCISP and the Intelligence Process

Guideline 1

Adhere to the *National Criminal Intelligence Sharing Plan* (NCISP) and perform all steps of the intelligence process.

Justification

After the tragic events of September 11, 2001, law enforcement executives and intelligence experts nationwide agreed that law enforcement agencies must work together toward a common goal of developing the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies. The *National Criminal Intelligence Sharing Plan* was developed in response to this need.

The NCISP provides model standards and policies, recommends methodologies for sharing classified reports, and recommends a nationwide sensitive but unclassified (SBU) communications capability for criminal intelligence sharing. The Plan is a living document that provides local, state, tribal, and federal law enforcement agencies the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence. It is the blueprint that law enforcement agencies can employ to support their crime-fighting and public-safety efforts while leveraging existing systems and networks. The Plan is not a system or a network, nor is it technology-based. It is the framework for the development and sharing of intelligence. It supports collaboration and fosters an environment in which all levels of law enforcement work together to improve the safety of our nation. The Plan and its related documents are a comprehensive reference guide for all law enforcement agencies.

The NCISP is founded on the concept of intelligence-led policing and encourages law enforcement agencies to embrace and integrate intelligence-led policing elements in their efforts. Intelligence-led policing provides a framework for law enforcement to work proactively instead of reactively. Intelligence-led policing has a number of benefits for law enforcement, such as the ability to:[19]

- Describe, understand, and map criminality and the criminal business process.
- Make informed choices and decisions.
- Engage the most appropriate tactics.
- Target resources.
- Disrupt prolific criminals.
- Articulate a case to the public and in court.

[19] Ronald Bain, "The Dynamics of Retooling and Staffing: Excellence and Innovation in Police Management," Canadian Police College, 2003.

The Intelligence Process

Criminal intelligence is the result of a process involving planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation of information on suspected criminals and/or organizations. This sequential process is commonly referred to as the intelligence process (or cycle). There are various models of the intelligence process in use; however, most models contain the basic steps depicted in the following graphic:

INTELLIGENCE PROCESS

The intelligence process is the means of developing raw information into finished intelligence products for use in decision making and formulating policies/actions. The first step, planning and direction, involves identifying the need for data. Agency members should engage in a process of deciding what they want to know (or what they need to collect) before they collect it, or they may obtain indiscriminate, unfocused information.

Collection is the gathering of the raw data needed to produce intelligence products. Data may be collected from many sources, including but not limited to public records, the Internet, confidential sources, incident reports, and periodicals.

The next step, processing and collation, involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined.

Analysis is the portion of the intelligence process that transforms the raw data into products that are useful. This is also the function that separates "information" from "intelligence." It is this vital function that makes the collection effort beneficial. Without this portion of the process, we are

left with disjointed pieces of information to which no meaning has been attached. The goal is to develop a report where the information has been connected in a logical and meaningful manner to produce an intelligence report that contains valid judgments based on information analyzed.[20]

Dissemination is also a vital step in the process. Without disseminating the intelligence developed, it is pointless to collect it. The intelligence disseminated must be timely and credible to be useful. Dissemination must also be evaluated based on a "right to know" and the "need to know." The right to know means the recipient has the legal authority to obtain the information pursuant to court order, statute, or decisional law. The need to know means the requestor has the need to obtain information to execute official responsibilities.[21]

The final step of the intelligence process involves evaluation/reevaluation of the process performed and the products produced by the intelligence function. In addition, evaluation/reevaluation assesses current and new information, assists in developing an awareness of possible weak areas as well as potential threats, and strives to eliminate previously identified weaknesses that have been hardened as a result of the fusion process. Overall, this step provides an opportunity to review the performance or effectiveness of the fusion center's intelligence function.[22]

As indicated previously, fusion centers have emerged as effective and efficient mechanisms for improving law enforcement's ability to fight crime and terrorism. Ensuring that each step within the intelligence process is followed will facilitate the production of useful intelligence products from fusion centers. Further, the fusion process, through managing the flow of information and intelligence across all levels and sectors of government, integrates the intelligence process to accomplish this function. The intelligence process provides a framework for the fused information to be turned into intelligence.

Often gaps in the intelligence process exist. To assist in closing these gaps, the FBI developed a template to assist agencies in identifying and tracking intelligence gaps. A summary of the FBI's Intelligence Requirements and a copy of the template can be found in *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Carter, November 2004).[23] A copy of this guide is included on the Resource CD. It is recommended that fusion centers create a formal intelligence and information requirements process that prioritizes and guides the intelligence function.

---

[20] Bob Morehouse, "The Role of Criminal Intelligence in Law Enforcement." Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., 2000, pp. 1-12.

[21] Ibid, p. 9.

[22] *The National Criminal Intelligence Sharing Plan*, 2003, p. 7.

[23] This information is available on the Community Oriented Policing Service (COPS) Web site at www.cops.usdoj.gov/Default.asp?Item=1404.

Issues for Consideration

When implementing portions of the NCISP, consider these steps to help establish or enhance an intelligence component of a fusion center:

1. *Recognize your responsibilities and lead by example.*
2. *Establish a mission statement and a policy to address developing and sharing intelligence data within your agency.*
3. *Connect to your state criminal justice network and regional intelligence databases and participate in information sharing initiatives.*
4. *Ensure privacy issues are protected in policy and practice.*
5. *Access law enforcement Web sites, subscribe to law enforcement listservs, and use the Internet as an information resource.*
6. *Provide your agency members with appropriate training on the criminal intelligence process.*
7. *Become a member in your regional RISS center.*
8. *Become a member of the FBI's LEO.*
9. *Partner with public and private infrastructure sectors.*
10. *Participate in local, state, and national intelligence organizations.*
11. *Consider participating in DHS's HSIN Program.*

Available Resources on Fusion Center CD

- 10 Simple Steps—to help your agency become a part of the *National Criminal Intelligence Sharing Plan*
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*
- *National Criminal Intelligence Sharing Plan* report

Mission Statement and Goals

Guideline 2

Collaboratively develop and embrace a mission statement and identify goals for the fusion center.

Justification

A mission statement is a written statement of the organization's purpose(s), such as enhancing public safety, sharing information, and/or resolving criminal investigations. It is important to have a mission statement because it focuses efforts; it is the foundation of all the decisions that follow. Many organizations use mission statements for internal and external purposes. A mission statement creates a common purpose that assists in coordinating decisions and actions. A mission statement can also inspire people in the organization and inform customers of the benefits and advantages of what the organization offers. The mission statement is the first step in educating entities about the center and its services.

If the center loses sight of its mission, it has lost focus of its overall purpose. If a center has a clear understanding of its short- and long-term goals, it will be easier to integrate efforts. Goals are what you want to accomplish. Objectives are how you are going to get there. Goals should be measurable and observable. They should have specific achievable steps (objectives) with built-in accountability for accomplishment. Goals should be high enough to challenge the center but realistic enough to be attainable. Universal law enforcement goals include four major desired outcomes:

1. The reduction of the incidence of crime.
2. The suppression of criminal activity.
3. The regulation of noncriminal conduct.
4. The provision of services.[24]

Fusion centers will have many demands placed on them, and it is important to have clear priorities. For example, in order to properly develop a mission statement and goals, centers should prioritize tasks such as analytical services, homeland security issues, and investigative support.

Issues for Consideration

When creating a mission statement and goals, consider:

- *Developing the center mission statement and goals collaboratively with participating entities—this will create ownership and assist in identifying the primary role(s) of the organization.*

[24] www.communitypolicing.org/goal.html.

- *Identifying center customers and their needs and defining center priorities prior to drafting the mission statement and goals.*
- *Prioritizing the intelligence function to address threats posed in specific fusion center jurisdictions.*
- *Integrating intelligence-led policing to support customer needs, define tasks, and prioritize functions.*
- *Utilizing vision statements and/or guiding principles to focus efforts.*
- *Using the center mission to lobby on behalf of the organization and support grant requests and funding.*
- *Including the mission statement in the MOU (see Guideline 5)*

Elements of Mission Statements

Mission statements should be clear and concise. They should include the primary purpose, priority, and roles of the center. Mission statements should communicate the essence of the organization so that stakeholders and the public are clear on the purpose and intent of the center. Ensure that the mission statement includes the name of the agency or organization, the type of agency, what the agency does, and whom the agency serves. It is critical that the appropriate time and commitment be placed on developing an adequate mission statement. A good mission statement will provide strategic vision and direction for the center.

Once the mission statement is created and approved, it should not require revision very often. The goals and objectives developed by the center should all be linked to the mission statement. These will be the short-term measures used to gauge whether the center is fulfilling the stated mission. However, if the mission statement becomes inappropriate, irrelevant, or outdated or if direction changes, the center should revise the mission statement accordingly.

Example Mission Statements

Upstate New York Regional Intelligence Center (UNYRIC)
To advance the efficient, timely, and accurate exchange of information between all New York state law enforcement agencies. The UNYRIC focuses on all aspects of criminal activity in the 54 counties outside the New York City area and interacts with law enforcement agencies nationwide.

Arizona Counter Terrorism Information Center (ACTIC)
To protect the citizens and critical infrastructures of Arizona by enhancing and coordinating counterterrorism intelligence and other investigative support efforts among local, state, and federal law enforcement agencies.

Rockland County Intelligence Center (RCIC)
To provide intelligence to law enforcement agencies based upon the collection, evaluation, and analysis of information that can identify criminal activity. This intelligence can be presented in the form of:

1. Strategic intelligence, which addresses existing patterns or emerging trends of criminal activity.
2. Tactical intelligence, which pertains to a specific event that can be used immediately.

Georgia Information Sharing and Analysis Center (GISAC)
To serve as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence relating to Georgia.

State Terrorism Threat Assessment Center (STTAC)—California
STTAC is designed to coordinate the collection of anti-terrorism intelligence data, the dissemination of that intelligence to law enforcement agencies, and the use of anti-terrorism intelligence resources.

Sample Mission Statements

The following are sample templates that centers may use when developing a mission statement:

The fusion center is a law enforcement [public safety] partnership, consisting of local, state, tribal, and federal agencies that acts as an information sharing gateway with the intent to assist law enforcement [homeland security agencies or agencies tasked with homeland security functions] to detect, prevent, and solve crimes.

The fusion center is a law enforcement [public safety] partnership among local, state, tribal, and federal agencies that collects, evaluates, analyzes, and disseminates information and intelligence to the law enforcement community [homeland security agencies or agencies tasked with homeland security functions] in a timely, effective, and secure manner.

Available Resources on Fusion Center CD

- *The Community Policing Consortium – Staircase to Strategic Planning: Mission* www.communitypolicing.org/mission.html

This Page Is Left Blank Intentionally

Governance

Guideline 3

Create a representative governance structure.

Justification

According to DOJ, governance is defined as the set of organizational regulations and standards exercised by management to provide strategic direction and ensure objectives are achieved, risks are managed appropriately, and resources are used responsibly.[25] Establishing a governance structure creates a supported environment that frames the ability for the center to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy. Governance creates a centralized body to review and endorse issues affecting operations. Members acting as the governance body are ambassadors to the program and carry the message to their agencies and constituents. Governance provides a forum for participants to voice concerns, offer suggestions, and make decisions. It enhances relationships, increases effectiveness, and provides leadership and cohesiveness among participants.

The governance structure ensures an equal opportunity for all participating agencies and users to have ownership in the decision-making process. Through the governance structure, agencies can strategically plan for center operations and future enhancements, as well as identify obstacles and offer resolutions.

Issues for Consideration

When creating a governance structure, consider:

- *Allowing participants to have input in the establishment of a governance structure.*
- *Collaborating with the JTTF, Attorneys General's Anti-Terrorism Advisory Council (ATAC), DOJ, DHS, and other state entities, local authorities, and other relevant entities to establish process.*
- *Comprising the governing body with high-level officials who have the power and authority to commit their respective agency's resources and personnel to the center.*
- *Defining the management structure to include what entity oversees the centers, manages the operations, and coordinates daily activities.*
- *Maintaining a governance structure that is reasonable in size yet ensures representation of all agencies that comprise the center.*
- *Creating an effective and timely mechanism to communicate decisions made by the governing body to participants and center personnel.*
- *Evaluating how political issues and climate may impact center support and operations.*

[25] OJP Web site, www.it.ojp.gov.

- *Establishing operational and technical committees.*
- *Developing bylaws for operations of the governance structure.*

Committees

Governing bodies may employ committees to assist in executing and adhering to the policies and procedures of the center, as well as to identify, review, develop, and/or implement new programs or policies. Executive committees set policy, make critical decisions, and commit resources. Operational committees may be asked to focus on specific policies, such as purge and retention or privacy. These types of committees may be asked to develop funding strategies or identify grant opportunities. Technical committees focus on technical standards, infrastructure, and security. Under these committees, subcommittees may be used to conduct detailed research and analysis, ultimately to bring recommendations to the governing body for review and endorsement.[26]

Example Governance Structures

In an effort to provide examples of governance structures, current initiatives were reviewed. The following is a selection of example governance structures.

Rockland County Intelligence Center (RCIC)
The RCIC Oversight Committee is comprised of police chiefs chosen by the Rockland County Police Chiefs Association (local representatives) and the Rockland County Sheriff and Rockland County District Attorney (county representatives). The Oversight Committee consists of three local representatives and two county representatives.

Iowa Law Enforcement Intelligence Network (LEIN)
Iowa LEIN is governed by a seven-member executive board, six of whom are local law enforcement officers who are elected annually by their fellow LEIN members from across the state. The seventh member and chairperson of the executive board is the state LEIN coordinator (a special agent with the Iowa Department of Public Safety's Intelligence Bureau).

State Terrorism Threat Assessment Center (STTAC)—California
STTAC represents a partnership among local, state, and federal law enforcement agencies pursuant to an MOU between the Governor and the Attorney General of California. The Executive Advisory Group, comprised of 16 members appointed by the Governor, provides program guidance.

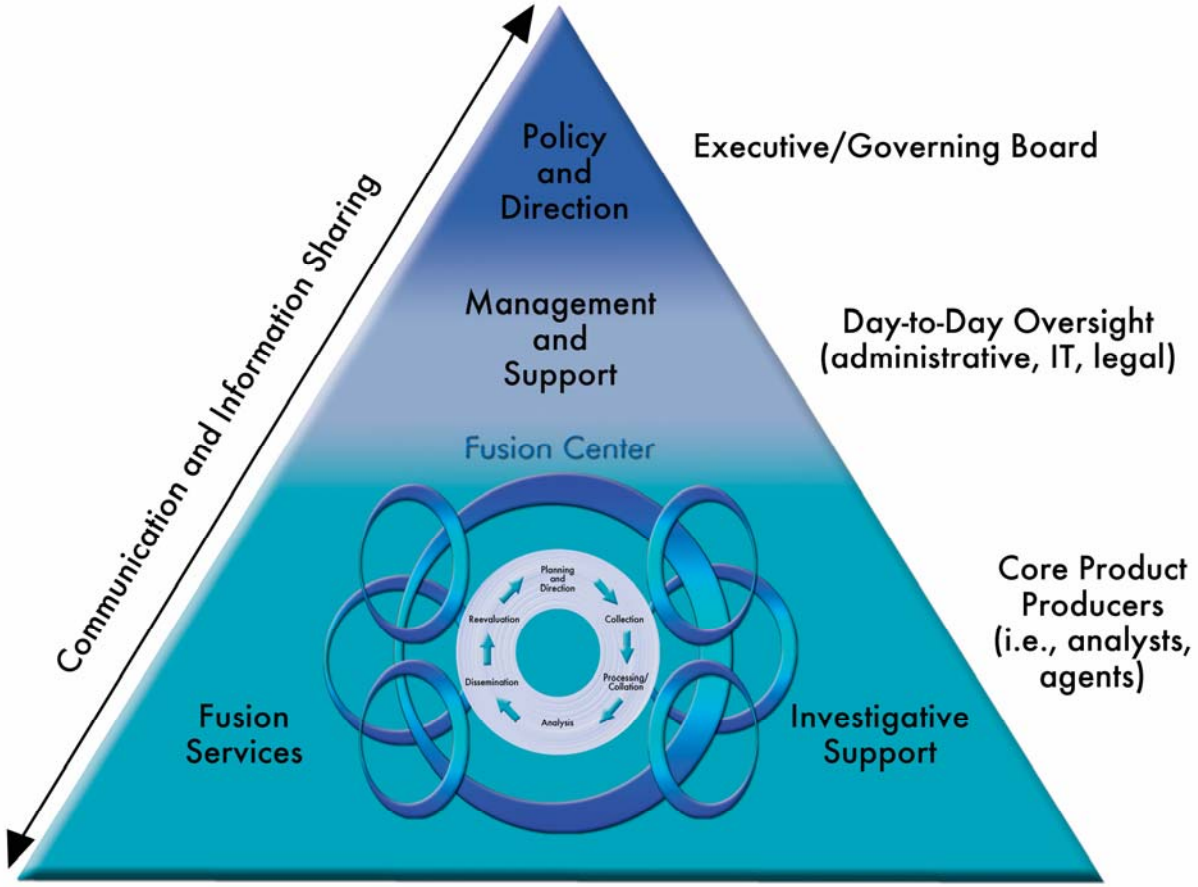
Governance Template

In an attempt to offer centers a starting point for developing a governance structure, the following example was developed. Figure 3 illustrates a three-tiered approach. The bottom level represents staff members assigned to perform the fusion/intelligence process and provide investigative support. These members may come from a variety of agencies and represent the core of center

[26] Kelly J. Harris, *Governance Structures, Roles and Responsibilities*, September 2000 (Updated/Reissued 2004).

operations. Here, data integration and analysis will take place. Personnel may include intelligence analysts and officers. The middle section represents the day-to-day management of the center. It also includes administrative staff, such as computer support staff and legal services. In some cases, this section may include a facility manager. The top section represents policy and direction. This section is smaller, indicating a selected group of individuals from each participating entity who have been designated as part of the governing structure or board. The illustration shows information flowing top down and bottom up.

Figure 3 – Fusion Center Governance Structure Example



Developing Bylaws

According to *The Legal Guide for Association Board Members*, bylaws are defined as "an important association corporate legal document that constitutes the agreement between the association and its members. Properly drafted bylaws set forth the essential organizational and operational provisions governing the association."[27] In other words, bylaws set out the rules by which

[27] James G. Seely, *The Legal Guide for Association Board Members*, Schneider, 1995, p. 71.

the organization is governed. Bylaws are just one example of a governing mechanism that a center may utilize to enforce organizational rules. A bylaws sample document is provided on the Resource CD.

Parliamentary Procedures

The fusion center governance board may want to make use of parliamentary procedures in order to create an effective governing process. Procedures such as *Robert's Rules of Order* can be very helpful in introducing, debating, and deciding on issues. There are a number of Web sites available containing the full text and/or summary information regarding *Robert's Rules of Order* and parliamentary procedures, such as www.rulesonline.com.

Available Resources on Fusion Center CD

- Bylaws Sample Template
- Board Guidelines, www.mapnp.org/library/boards/boards.htm
- Global Justice Information Sharing Initiative Advisory Committee bylaws, http://it.ojp.gov/documents/GACBylaws.pdf
- Parliamentary Procedures, www.rulesonline.com

Collaboration

Guideline 4

Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies.

Justification

In order to maximize intelligence sharing, it is critical that law enforcement agencies at all levels communicate and collaborate, thereby leveraging resources and expertise while improving the ability to detect, prevent, and apprehend terrorists and other criminals. Fostering a collaborative environment builds trust among participating entities, strengthens partnerships, and provides individual as well as a collective ownership in the mission and goals of the center. The *National Criminal Intelligence Sharing Plan* speaks to this as well: ". . . . sharing is founded upon trust between the information provider and the intelligence consumer. Such trust is most often fostered on an interpersonal basis; therefore, law enforcement task forces and other joint work endeavors succeed where colocated, interspersed personnel from different agencies and job types convene for a common purpose."[28]

Fostering a collaborative environment is not only important to share, collect, develop, and disseminate intelligence but also to share decisions and ownership. It discovers solutions and expands capacity. In an environment where some resources are decreasing while demands are increasing, collaboration has become even more essential. The purpose of collaboration is to increase capacity, communication, and continuity of service while decreasing duplication.[29]

Collaboration Principles

To ensure that the collaboration is successful, it must continually provide value to its participants, customers, and constituency. To foster and enhance collaboration, consider implementing the following principles:

- *Maintaining a diverse membership to include representatives from local, state, tribal, and federal law enforcement.*
- *Developing and participating in networking groups and organizations that exist locally, regionally, statewide, nationally, and internationally.*
- *Working with JTTF, ATAC, DOJ, DHS, other state and local entities, and other relevant organizations or groups.*
- *Conducting regular meetings for the purpose of collaboration and information sharing.*

[28] *National Criminal Intelligence Sharing Plan,* November 2004, p. 9.
[29] C. R. Pete Petersen, M.Ed., "Community Collaboration," March 4, 2003, www.communitycollaboration.net.

- *Establishing procedures for maintaining the continuity of personal, organizational, and institutional relationships.*
- *Educating and training the law enforcement community on the intelligence process and fusion center operations.*
- *Educating and liaising with elected officials and other community leaders to promote awareness of the fusion center functions.*

Available Resources on Fusion Center CD

- Community Collaboration, www.communitycollaboration.net

Memorandum of Understanding (MOU)

Guideline 5

Utilize MOUs or other types of agency agreements, as appropriate.

Justification

It is recommended that fusion centers be governed and managed in accordance with an MOU. An MOU is a necessary tool for information sharing efforts. MOUs define the terms, responsibilities, relationships, intentions, and commitments of each participating entity; the agreement provides an outline of the who, what, where, how, why, and when of the project. Partners shall commit to the program policies by signing the MOU. In addition to MOUs, some initiatives utilize agency, individual, and data sharing user agreements.

Issues for Consideration

When negotiating and drafting MOUs, consider:

- *Identifying and understanding the legal and practical implications of the MOU.*
- *Defining the roles and responsibilities of the participating agencies.*
- *Embracing and encouraging trusted relationships.*
- *Including language requiring that all assigned personnel maintain access to their own agency's data.*

Example MOUs

At a minimum, include the following elements in the MOU:

- Involved parties
- Mission
- Governance
- Authority
- Security
- Assignment of personnel (removal/rotation)
- Funding/costs
- Civil liability/ indemnification issues
- Policies and procedures
- Privacy
- Terms
- Integrity control
- Dispute resolution process
- Points of contact
- Effective date/duration/ modification/termination
- Services
- Deconfliction procedure
- Special conditions
- Protocols for communication and information exchange

Available Resources on Fusion Center CD

- 28 CFR Part 23 Sample MOU
- Arizona Counter Terrorism Information Center MOU
- Canada Department of Defense (DOD) MOU Guidelines
- Joint Terrorism Task Force MOU
- MOU Sample Template
- Rockland County Intelligence Center MOU
- Upstate New York Regional Intelligence Center MOU

Database Resources

Guideline 6

Leverage the databases and systems available via participating entities to maximize information sharing.

Justification

During the focus group process, participants reviewed a number of information and intelligence sharing initiatives. Most of the initiatives have access to some local, state, and federal databases as well as other organizations or data sets. Centers may want to evaluate the types of databases that participating agencies have available. Gaps should be identified and researched. Leveraging the databases and systems available via participating entities will help maximize information sharing. This is an opportunity to access information previously unavailable. It is recommended that ownership and control of law enforcement information shared through the center remain with the initial originating agency. Data owners should be responsible for the quality of data shared. Another option pertains to the center housing their information. If a center chooses this option, it is important for the necessary policies and procedures to be in place to govern use, access, etc.

Issues for Consideration

When accessing databases, consider obtaining access to a variety of databases and systems, such as:

- *Driver's license*
- *Motor vehicle registration*
- *Location information (411, addresses, and phone numbers)*
- *Law enforcement databases (National Crime Information Center [NCIC], NLETS – The International Justice and Public Safety Information Sharing Network, and the Terrorism Screening Center [TSC])*
- *Criminal justice agencies*
- *Public and private sources*
- *RISS/LEO, HSIN (Note: RISS, LEO, and HSIN are currently collaborating on a network capability)*
- *Corrections*
- *Sex offender registries*
- *Violent Criminal Apprehension Program (VICAP)*

Also important is the consideration of issues, such as:

- *Classification of data (security levels)*
- *Technical specification of your database (structured/unstructured data)*

- *Identification and leveraging of partner resources*
- *Ownership of the data in the fusion center*
- *Data quality and data reliability*

System/Network Resources

The following are available resources for law enforcement entities. **This list is not meant to be all inclusive. Additional resources and Web sites may exist to assist law enforcement.**

El Paso Intelligence Center (EPIC) – EPIC established a Southwest Border Intelligence Service Center with a concentration on drug movement and immigration violations. Members of EPIC have access to a wide range of intelligence, including information from the U.S. Drug Enforcement Administration and Immigration and Customs Enforcement. www.usdoj.gov/dea/programs/epic.htm

FBI's LEO Program – LEO is a national, interactive computer communications system and information service, an intranet exclusively for the law enforcement community. www.fbi.gov/hq/cjisd/leo.htm

FBI's R-DEx – R-DEx provides an interface to Regional Intelligence Centers (RICs) to enable searching of unstructured documents and for retrieving matching documents. R-DEx serves two main functions: providing RICs with access to DOJ's data and enabling a RIC's user to perform full-text searches over DOJ unstructured documents for the region, in addition to the state and local documents accessed internally.

FBI's N-DEx – N-DEx will provide the first implementation of structured search and index for DOJ's Law Enforcement Information Sharing Program. All kinds of data (structured, full-text, multimedia, etc.) will be available through N-DEx, although searching, matching, and linking will only be possible on well-defined entities (people, vehicles, locations, weapons, phone numbers, etc.), not arbitrary text (full-text data). The initial focus is on structured incident data but will be expanded to other structured data (extracted entity data from full-text documents). N-DEx's focus is on large agencies and aggregated data sources such as RICs but will expand to any law enforcement agency.

Financial Crimes Enforcement Network (FinCEN) – FinCEN supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes to provide United States policymakers with strategic analysis of domestic and worldwide money-laundering developments, trends, and patterns. FinCEN controls over 150 million reports filed under the Bank Secrecy Act and other similar laws. www.fincen.gov

High Intensity Drug Trafficking Areas (HIDTA) – This program provides federal funds to problem areas to help eliminate or reduce drug trafficking and its harmful consequences. Analysts at HIDTA centers have access to a variety of databases and systems that are available to law enforcement. www.whitehousedrugpolicy.gov/hidta/index.html

Homeland Security Information Network (HSIN) – HSIN provides an Internet-based secure technology that allows real-time information sharing at the sensitive but unclassified level. HSIN is

the secure collaborative system used by the U.S. Department of Homeland Security's (DHS) Operations Center to collect and disseminate information between DHS and local, state, tribal, and federal agencies involved in combating terrorism. HSIN also includes private sector connectivity, homeland security, and other information. Access to Secret Information will be available in the near future on HSIN-Secret. www.dhs.gov/dhspublic/display?content=3350

International Association of Crime Analysts (IACA) – IACA helps crime analysts around the world improve their skills and make valuable contacts, helps law enforcement agencies maximize use of crime analysis, and advocates for standards of performance and technique with the professions. www.iaca.net

International Association of Law Enforcement Intelligence Analysts (IALEIA) – IALEIA's mission is to professionalize analysis in law enforcement, military, and private industry. IALEIA holds major conferences, local or regional chapters meetings, and training sessions and has published a number of booklets. www.ialeia.org

International Criminal Police Organization (INTERPOL) – INTERPOL is a worldwide law enforcement organization established for mutual assistance in the prevention, detection, and deterrence of international crimes. It houses international police databases, provides secure international communications between member countries for the exchange of routine criminal investigative information, and is an information clearinghouse on international criminal/fugitives and stolen properties. www.usdoj.gov/usncb/

Law Enforcement Intelligence Unit (LEIU) – The purpose of LEIU is to record and exchange confidential criminal information not previously available through regular police communication channels concerning organized crime. Membership in LEIU is open to local or state law enforcement agencies having a criminal intelligence function. The applicant must be sponsored by a current member. LEIU may be reached at the State Terrorism Threat Assessment Center, Bureau of Investigation, Intelligence Operations Program, Central Coordinating Agency, Post Office Box 163029, Sacramento, CA 95816-3029. www.leiu-homepage.org/main.cgi

National Crime Information Center (NCIC) – NCIC is a nationwide information system that links local, state, tribal, and federal criminal justice agencies together. NCIC's capabilities include an enhanced name search, fingerprint searches, information on persons on probation or parole, convicted sex offender registry, and a registry of individuals incarcerated in the federal prison system. www.fbi.gov/hq/cjisd/ncic.htm

National Drug Intelligence Center (NDIC) – The NDIC supports national policy and law enforcement decisions with timely strategic domestic drug intelligence assessments, focusing on the production, trafficking, and consumption trends and patterns of all illicit drugs inside United States national borders and territories. www.usdoj.gov/ndic

National White Collar Crime Center (NW3C) – NW3C provides a national support network for local and state law enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime. NW3C is a member-affiliated organization comprised of law

enforcement agencies, state regulatory bodies, and local and state prosecution offices. Support services are offered in five main categories: economic and computer crime training, intelligence and analytical services, case funding for designated cases, research, and fraud-compliant referral and analysis through its National Fraud Complaint Management Center/Internet Fraud Complaint Center. www.nw3c.org and www.training.nw3c.org

NLETS – The International Justice and Public Safety Information Sharing Network – NLETS is an interstate law enforcement network for the exchange of law enforcement and related justice information. http://64.132.171.113/index.asp

RISS Automated Trusted Information Exchange (ATIX) – RISS ATIX™ provides users with secure interagency communications and information sharing resources for exchanging public safety and law enforcement information. www.rissinfo.com/rissatix.htm

RISSNET™ – RISSNET provides the six RISS centers with a secure criminal intelligence network for communications and information sharing by local, state, tribal, and federal law enforcement agencies. www.rissinfo.com

Interconnectivity

Guideline 7

Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development and allow for future connectivity to other local, state, tribal, and federal systems. Use the Global Justice Extensible Markup Language (XML) standard for future database and network development.

Justification

It is imperative that law enforcement entities communicate. The ultimate goal is to eliminate the barriers that impede communications and intelligence development and exchange. Communication barriers come in a number of formats—incompatible or disparate computer systems, lack of trust, lack of interoperability, lack of a common terminology, and lack of funding. Centers should establish formal protocols (policies and procedures) to enhance communications as well as create effective and efficient vehicles for exchanging information. Center personnel and leadership should communicate frequently and be responsive to the needs, concerns, and ideas of both internal and external partners. The information contained in this guideline pertains to verbal, written, and electronic communications.

It is recommended that fusion centers leverage existing systems and those currently under development and allow for future connectivity to other state, local, tribal, and federal systems. Furthermore, it is recommended that centers be aware of and educated on Global Justice XML. Any new database development should be Global XML-compliant and meet existing standards. This component also includes the successful and secure transfer of data and information. It is important to note that DOJ and DHS are integrating XML into grant recipient criteria.

The Global Justice XML Data Model (Global JXDM) is a comprehensive product that includes a data model, a data dictionary, and an XML schema that together is known as the Global JXDM. The Global JXDM is sponsored by DOJ, with development supported by the Global XML Structure Task Force (GXSTF), which works closely with researchers at the Georgia Tech Research Institute (GTRI). The Global JXDM is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner. The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, Global JXDM enables access from multiple sources and reuse in multiple applications.

The Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ) is collaborating with the U.S. Department of Homeland Security (DHS) to utilize the Global JXDM as the base for the

deployment of the National Information Exchange Model (NIEM). NIEM will provide the foundation and building blocks for national-level interoperable information sharing and data exchange that will integrate the public safety and private sector entities to the already established law enforcement information exchange. The tentative date for NIEM to be operational is June 2006.[30]

Issues for Consideration

When establishing connectivity and communications, consider:

- *Striving for compatibility not commonality.*
- *Including both technical and managerial portions of connectivity.*
- *Using Web-enabled technology when available.*
- *Using a distributed structure when appropriate.*
- *Developing mechanisms to communicate internally with participating agencies.*
- *Developing a policy to ensure proper communications with leaders and policymakers, public sector, private sector, media, and citizens.*
- *Ensuring secure and redundant communications.*
- *Establishing an electronic notification capability for fusion center participants.*
- *Maintaining a stand-alone security system (mobile).*
- *Implementing a communications plan.*
- *Adhering to need-to-know/right-to-know stipulations.*
- *Developing outreach materials to help increase awareness among policymakers, media, and citizens.*
- *Conducting training on proper communications and center policy.*
- *Meeting regularly with personnel and offering intelligence exchange sessions.*
- *Remembering that communications go beyond just in-house communications.*
- *Incorporating the protocols for communication and information exchange in the MOU (Guideline 5)*

Distributed Versus Centralized Systems

There are currently both distributed and centralized systems being used successfully for law enforcement information and intelligence sharing. There are advantages and disadvantages to both models.

The use of a distributed model allows participating entities to maintain control of their data. Data is not commingled or housed in a data warehouse. Agencies are responsible for the quality of the data and the accessibility of their information. The distributed structure can streamline policy development and minimize privacy concerns, while providing the same functionality as a centralized model.

[30] For more information on NIEM, visit www.niem.gov.

The distributed model is also reliable and can maximize resources. Distributed systems are scalable and offer aggregate computer power. However, security issues, resource distribution, and demand as well as computing power can limit the distributed model.[31]

A centralized system places all information in one location. Collection of information and refreshing of data can be complicated with a centralized structure. Often, however, the functionality of the centralized system is greater and allows for increased speed.

A white paper prepared by the Integrated Justice Information Systems (IJIS) Institute provides a comparative analysis of the distributed and centralized system based on five components: cost, governance and data ownership, performance and functions, scalability, and security and privacy. This document is included in the Resource CD. It is important for centers to evaluate both structures to determine the best fit for their individual center needs.

Service-Oriented Architecture

Information sharing is a long-standing practice among justice agencies, particularly within the law enforcement community. As society becomes more mobile, the importance of sharing data to improve police effectiveness grows exponentially. The arrival of the World Wide Web (the Web) and the technologies that support it have spawned a brave new world of information sharing that goes beyond exchanges among specific partners to embrace the whole of the justice community—law enforcement, prosecutors, defense counsel, courts, probation, corrections—and a host of corollary disciplines, such as homeland security, fire, emergency services, health, education, transportation, and motor vehicle licensing. Service-oriented architecture (SOA) incorporates six fundamental principles for the sharing of information in the criminal justice community:

- The architecture must recognize innumerable independent agencies and funding bodies from local, state, tribal, and federal governments.
- Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.
- The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.
- Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.
- Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.
- The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

This concept of design allows the original data owners to control their own data, both in terms of who is allowed to access it and in ensuring the integrity of the data. It allows agencies to retain the investment they have made in their existing systems, while at the same time gain access to

[31] Texas A&M University Computer Science Department. Introduction to Distributed Systems, 2001.

valuable information contained in other agency systems. It uses the technology of the Internet, which is user-friendly and readily understood by most users of today's computer systems.

On September 28, 2004, the Global Infrastructure/Standards Working Group (GISWG) published a document entitled ***A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)***. Based on the report, Global recognizes that SOA is the recommended framework for development of a justice information sharing system. The report indicates that a system should be designed and developed around the basic components of the operational procedures or business practices of an agency. These components are then combined into a loosely related larger structure that, in turn, can be combined into an even larger entity. The SOA design must be available to all agencies and support the evolution of change and new technology. Funding must be available for start-up, maintenance, and future upgrades to the information sharing systems that are based on the SOA framework. A complete copy of the report is contained on the accompanying Resource CD.

Organization for the Advancement of Structured Information Sharing Systems (OASIS)—Ratified Common Alerting Protocol (CAP)

It is recommended that, where possible, fusion centers use the OASIS-ratified CAP to enable the exchange of emergency alert and public warning information over data networks and computer-controlled warning systems. Using CAP also adds an element of redundancy in the systems and networks. By limiting transport-specific nomenclature, CAP remains fully compatible with existing public warning systems, including those designed for multilingual and special-needs populations, as well as with XML applications, such as Web services. CAP data elements have been incorporated in DOJ's Global JXDM. Other agencies, such as DHS's Federal Emergency Management Agency (FEMA), have embraced the CAP and are in the process of integrating it into all current and future alert and warning systems.

Available Resources on Fusion Center CD

- *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA),* http://it.ojp.gov/documents/200409_Global_Infrastructure_Report.pdf
- Model Intelligence Database Policy
- *A Critical Look at Centralized and Distributed Strategies for Large-scale Justice Information Sharing Systems* (a white paper prepared by the IJIS Institute)
- Global Justice XML Data Model (Global JXDM), www.it.ojp.gov/gjxdm

Privacy

Guideline 8

Develop, publish, and adhere to a privacy and civil rights policy.

Justification

The NCISP stresses the importance of the need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process. The NCISP also noted that one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals' privacy and constitutional rights through the use of intelligence sharing systems. In order to balance law enforcement's ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place. The privacy design principles (also known as the Fair Information Practices), as outlined in the National Criminal Justice Association (NCJA) document *Justice Information Privacy Guideline,* provide assistance when developing a privacy policy and identifying privacy issues. The fusion center should take steps to incorporate applicable local, state, and federal privacy laws into their fusion center privacy policy. The following is a summary of the Fair Information Practices:

1. Collection limitation principle. There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

3. Purpose specification principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation principle. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with paragraph 3 except (a) with the consent of the data subject or (b) by the authority of law.

5. Security safeguards principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

6. Openness principle. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation principle. An individual should have the right to (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; (c) be given reasons if a request made under (a) and (b) is denied and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. Accountability principle. A data controller should be accountable for complying with measures that give effect to the principles stated above.

The NCISP recommends that privacy policies should:

- Eliminate unnecessary discretion in the decision-making process, guide the necessary discretion, and continually audit the process to ensure conformance with the policy goals.
- Ensure legitimacy—when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented.
- Clearly define the parameters of the policy.
- Acknowledge and address important issues that currently are not included in some existing criminal intelligence policies.
- Identify the decision points within the intelligence process and provide appropriate guidance and structure for each.

Issues for Consideration

Issues to consider when drafting a privacy policy include:

- *Adding introductory language that clearly states the privacy practices of the center.*
- *Describing the information collected and how information is stored.*
- *Establishing a common lexicon of terms for dealing with role-based access.*
- *Defining and publishing how the information will be used.*
- *Drafting a clear, prominent, and understandable policy. Avoid communicating in complicated or technical ways.*
- *Displaying the privacy policy for both center personnel and customers.*
- *Ensuring that all other policies and internal controls are consistent with the privacy policy.*
- *Establishing a business practice to notify government agencies of suspected inaccurate data.*
- *Partnering with training centers on privacy protection requirements and conducting periodic privacy security audits.*

Adhering to Privacy Policy

There are a number of mechanisms that centers can develop or establish that will assist them in adhering to their privacy policy. Some of these include:[32]

- Establish a privacy oversight committee or appoint a privacy officer.
- Develop or update privacy training and orientation for all employees.
- Develop a mechanism for ongoing information privacy awareness.
- Establish a process for tracking and handling privacy complaints or concerns.
- Develop a consistent sanction policy for failure to comply with the privacy policy for all individuals in the organizations.
- Recognize the overlap and coordinate privacy activities with security activities within the organization.
- Ensure all center personnel are adequately trained on the privacy policy.
- Consult legal counsel.

Available Resources on Fusion Center CD

- Audit Checklist (LEIU), www.it.ojp.gov/documents/LEIU_audit_checklist.pdf
- *Global Privacy and Information Quality Policy Development for the Justice Decision Maker,* http://it.ojp.gov/documents/200411_global_privacy_document.pdf
- National Criminal Justice Association—Justice Information Privacy Guideline, www.ncja.org/pdf/privacyguideline.pdf
- Privacy Policy Sample Template

[32] Beth Hjort, "A HIPAA Privacy Checklist (AHIMA Practice Brief)," *Journal of AHIMA 72*, Number 6, 64A-C, 2001.

This Page Is Left Blank Intentionally

Security

Guideline 9

Ensure the appropriate security measures are in place for the facility, data, and personnel.

Justification

Security pertains to the implementation of policy related to information, documents, databases, facility, and personnel. Security measures such as authorization, encryption, access control, and confidentiality are critical to protect the security and integrity of information collected and shared. In determining how most appropriately to protect data, there are many policy and technical issues for data owners to consider. It is important that policy issues be decided before technical issues are developed.

Facility and personnel security should also be a part of the center's security plan. Appropriate security clearances should be obtained for personnel within the fusion center and key decision makers who need access. Security plans should be marked, handled, and controlled as sensitive but unclassified information. Some questions to consider when developing a security policy and plan include, but are not limited to:

- Who does the data owner want to have access?
- How should users access data?
- What access methods are necessary for the users' jobs?
- Should audits be used to ensure proper use of data?
- Should centers conduct background checks on personnel?
- What security needs exist for the facility?
- What security is needed for the data?
- Should a system-logging mechanism be utilized?

Issues for Consideration

When developing security protocols, consider:

- *Adopting established models for secure information and intelligence sharing such as the RISS, LEO, R-DEx, and HSIN.*
- *Addressing limited/restricted access, authorization, authentication, and encryption.*
- *Applying security policies to both physical and electronic forms of information.*
- *Using Applying Security Practices to Justice Information Sharing.*
- *Determining access levels and maintaining a policy on the level of information released.*
- *Verifying access based on criteria established by governance structure.*
- *Creating a form to be submitted by the agency authorizing access/supervisory approval.*

- *Conducting background checks on personnel.*
- *Considering applicable security guidelines for access control.*
- *Considering relevant security clearances.*
- *Creating and providing a training component on center security protocols.*
- *Utilizing relevant local, state, and federal building security requirements.*
- *Utilizing relevant portions of 28 CFR Part 23 as it relates to security.*
- *Appointing a privacy officer as a central point for compliance and oversight.*

Centers may also consider maintaining a security officer who would be responsible for evaluating and providing information about the security program to management and communicating security requirements and concerns to the organization. The security officer would conduct security training and awareness and prepare a policy on security. Any breach issues would be reported to and investigated by the security officer. Consideration should be given to colocating with other Intelligence Centers such as HIDTA or other law enforcement facilities in order to share security responsibilities.

Applying Security Practices to Justice Information Sharing provides details on how to safeguard critical elements of information sharing initiatives, as well as the infrastructure and integrity of data, systems, facilities, and personnel. According to the document, the following issues should be considered when developing and adhering to security policies:

- Identify potential physical threats to departmental computer systems and networks.
- Establish policies and procedures to thwart potential physical threats.
- Conduct audits to monitor employee compliance with department policies and procedures.
- Consider including the following physical security policies in the organization's overall security policy:
  - Identify unauthorized hardware attached to the department computer system; make routine checks of system hardware for unauthorized hardware.
  - Limit installation of hardware and software owned by employees on department desktop workstations.
  - Identify, tag, and inventory all computer system hardware.
  - Conduct regular inspections and inventories of system hardware.
  - Conduct unscheduled inspections and inventories of system hardware.
  - Implement policies that instruct employees/users on how to react to intruders and how to respond to incidents where an intrusion has been detected.
- Require background checks on all employees every five years.

Federal regulation 28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded, multijurisdictional criminal intelligence systems, and it provides the following guidelines regarding security:

- The database, manual or electronic, shall be located in a physically secured area that is restricted to designated authorized personnel.

- Only designated authorized personnel will have access to information stored in the database.
- All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility and physical location housing the database.
- All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- All hard-copy submissions and/or manual files will be secured by lead agency-designated authorized personnel when not being used and at the end of each shift.
- Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access will be adopted.
- When direct remote terminal access is authorized by participating agencies, policies and procedures addressing the following additional security measures shall be adopted:
  - Identification of authorized remote terminals and security of terminals.
  - Identification and verification of authorized access officer (remote terminal operator).
  - Levels of dissemination of information as directed by the submitting agency.
  - Rejection of submissions unless critical data fields are completed.
  - Technological safeguards on access, use, dissemination, and review and purge.
  - Physical security.
  - Training and certification of participating agency personnel.
  - Audits and inspections of participating agencies, including file data-supporting submissions, security of access terminals, and policy-and-procedure compliance.
  - Documentation for audit trails of the entire operation.

Available Resources on Fusion Center CD

- *Applying Security Practices to Justice Information Sharing,* http://it.ojp.gov/documents/asp/introduction/index.htm
- National Institute of Standards and Technology (NIST) template and example policies, http://csrc.nist.gov/fasp
- *Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs,* U.S. Department of Homeland Security, May 2005

This Page Is Left Blank Intentionally

Facility, Location, and Physical Infrastructure

Guideline 10

Integrate technology, systems, and people.

Justification

Ensuring that participants are integrated is a key element of the fusion center. It is important to bring technology, systems, and people together. Integrating these components streamlines operations, creates an effective and efficient environment, and increases productivity. There are a number of ways to integrate participants. Two options are presented for consideration—colocating and virtual integration. Colocating personnel in one facility is the preference.

Colocating participating entities improves communications and breaks down barriers that hinder operations. Often, lack of resources and/or funding can impede the ability to colocate. However, it is recommended that participating agencies strive to locate personnel in the same facility, when possible. Colocation consolidates resources and equipment. In addition, it fosters an environment to develop and exchange information and intelligence.

If colocating is not a feasible option for a fusion center, participating entities may consider virtual integration, linking the information sharing and communications systems so personnel can seamlessly access and exchange information. Fortunately, technology has improved greatly over the years and continues to generate new and innovative capabilities. Virtual integration can be an effective technology solution for integrating personnel and processes.

Regardless of the option a fusion center chooses, it is important to ensure flexibility and scalability, allowing for each step of the intelligence process to be conducted.

Issues for Consideration

The Fusion Center Intelligence Standards Focus Group preferred that participating entities be colocated. However, they also recognized the logistical issues and obstacles affecting the ability to colocate. In addition, the focus group recognized that not colocating also has benefits, such as the ability for mobile capacity, contingency operations during emergencies, and flexibility in offering services and support. There are a number of logistical issues that must be addressed when deciding on a facility and location for a fusion center. The primary issues, which are not in priority order, include:

- *Connectivity*
  - *Will the fusion center, emergency operations center, or other partners be connected? If so, how?*
- *Scalability*
  - *Ensure the facility allows for future and emergency expansion.*

- *Security*
  - *For the facility, data, personnel, and visitors (see Security [Guideline 9] for more information).*
- *Redundancy*
  - *Ensure redundancy for the infrastructure, resources, personnel, systems, etc.*
- *Emergency Power*
- *Continuity of Operations Plan (COOP)*
- *Threat/Vulnerability Assessments*
- *Political Issues*
  - *Recognize that the political climate will be different for each center.*
  - *Work with and inform political officials and policymakers regularly.*
- *Access*
  - *Ensure center personnel have seamless access to each other.*
- *Personnel*
  - *Ensure full and equal representation at local, state, and federal levels.*
- *Authority/Regulations*
  - *Follow appropriate policy, statutes, Concept of Operations (CONOPS), and other guidelines.*
- *Roles and Responsibilities*
  - *Clearly define personnel responsibilities, including roles during emergency situations.*

Site Selection

When selecting or building a site for a fusion center, it is important for the site to be based on the functional needs of the center. At a minimum, a site should be designed based on the following functional elements:

- Collection/Data Management
- Analysis
- Command and Control/Executive
- Deconfliction
- Communication and Dissemination
- Facilities Management
- Feedback

If the center plans on managing multiple sites, additional consideration should be made toward connectivity and collaboration issues.

The following list contains some key components to assist agencies in developing a plan to locate, acquire, and/or renovate a facility:

- Identify facility needs.
- Identify a facility project team to manage facility issues.
  - Ensure that center personnel are involved in site selection.
- Communicate with center leadership.
- Identify and secure needed funding (see Funding [Guideline 17] for more information).
- Conduct a space-needs analysis.

- Utilize existing resources when possible.
- Conduct a security/infrastructure assessment.
- Evaluate facility operations.
- Conduct site visits.
  - Consider geographical and environmental issues as well as convenience and location.
- Develop transition plan and timetable for occupancy.
- Work with technical personnel to ensure connectivity and security issues are established.
- Train staff regarding facility, security measures, and policy requirements.
- Regularly evaluate the facility and conduct proper maintenance.

Physical Security

Physical security includes all elements that make up the facility. The goal of physical security is to protect people, property, and processes. In order to ensure physical security, centers should plan, identify, design, train, implement, and adhere to all appropriate security measures; identify and create a program that identifies physical assets, threats, and vulnerabilities; assess and prioritize risks; and identify ways to resolve and respond to concerns or breaches.[33] It is recommended that a physical security plan have, at a minimum, the following components:[34]

- Risk Assessment
- Operating Procedures
- Training, Testing, and Rehearsal Plan
- Managing Threats
- Communications Plan
- Occupant Emergency Plan (OEP)
- COOP

Centers may consider maintaining a facility/security manager or officer who is responsible for preparing the facility security policy, monitoring and adhering to the policy, and training center personnel regarding the security policy and protocols. Training of users is critical. Users must understand their role and responsibility in adhering to a security plan as well as how to notify the appropriate management when issues or concerns arise regarding security, such as lost badges or noncompliance (see Security [Guideline 9] for more information).

Contingency Plan

The focus group also recommended that fusion centers identify a skeleton model for emergency operations. In other words, develop a contingency plan. The purpose of a contingency plan is to enable the sustained execution of mission-critical processes and information technology systems for the center during an occurrence of an extraordinary event that causes these systems to fail minimum production requirements. A contingency plan template can be found at the NIST Web site referenced on the Resources CD.

---

[33] David Hochman, *Disruption Defense: Facility Security Breaches*, 2002.
[34] General Services Administration, 3d ed., www.gsa.gov, 2004.

In addition, it is recommended that fusion centers develop and adopt a program for a COOP to perform essential functions at an alternate location during an emergency or other situation that may disrupt normal operations at the fusion center. COOP planning is designed to develop and maintain a plan that enables each level of government and jurisdiction to preserve, maintain, and/or reconstitute its capability to function effectively in the event of a threat, disaster, or emergency that could potentially disrupt operations and services. Consult DHS-FEMA's *Interim Guidance on Continuity of Operations Planning for State and Local Governments* dated May 2004.

Security Clearances

Most information needed by state or local law enforcement can be shared at an unclassified level. However, in those cases where it is necessary to share classified information, it can usually be accomplished at the "Secret" level. Resources regarding security clearances are included on the Resource CD.

Centers also need a secure operation to perform classified work. Centers may consider use of the Sensitive Compartmented Information Facility (SCIF) concept. An SCIF is defined as an accredited area, room, group of rooms, building, or an installation where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed. SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency.[35]

Available Resources on Fusion Center CD

- IACP Police Facility Planning Guidelines, www.iacp.org/documents/pdfs/Publications/ACF2F3D%2Epdf
- Executive Orders 12068, 12958, and 13292 regarding classified information
- FBI Security Clearance and Frequently Asked Questions

[35] Criminal Intelligence Glossary of Terms, November 2004.

Human Resources

Guideline 11

Achieve a diversified representation of personnel based on the needs and functions of the center.

Justification

Selecting personnel for the center depends upon the needs and functions of the center. It is anticipated that the center will conduct, at a minimum, all aspects of the intelligence process. Staff will need the ability to perform analytical functions and provide strategic and tactical assistance. It is important for the center to recruit the highest quality individuals and to ensure center personnel are assigned appropriately, based on the needs of the center. For example, center leadership should ensure qualified personnel are selected for key objectives, such as collection and analysis. It is recommended that center personnel be expected to demonstrate attention to detail, integrity, good interpersonal communication skills, and the ability to accept and learn from criticism. It is important to note that ensuring appropriate staffing is dependent upon available resources, funding, and support.

Issues for Consideration

When staffing a fusion center, consider:

- *Recruiting personnel based on a Concept of Operations (CONOPS) and center mission and goals.*
- *Maintaining a 24-hour-a-day/7-day-a-week operation with appropriate staffing levels.*
- *Ensuring appropriate command structure and leadership.*
- *Establishing a permanent full-time civilian position to provide continuity and consistency in the long term (i.e., facility manager/center director).*
- *Maintaining a small core staff dedicated to specific functions, such as administration, information technology, communications, and graphics.*
- *Creating units of operation (or crime desks) such as intelligence, criminal investigations (e.g., violent crimes, drugs, gangs), analytical, and homeland security.*
- *Identifying and utilizing subject-matter experts.*
- *Ensuring equal/proportional representation of personnel from participating entities.*
- *Maintaining legal counsel dedicated to the fusion center to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and liaison with the development of policies, procedures, guidelines, and operational manuals.*
- *Liaising with the local prosecutor's office.*
- *Securing appropriate number and types of security clearances for personnel and identifying clearances based on local, state, and federal requirements.*
- *Requiring a minimum term commitment for full-time center personnel (i.e., two years).*

- *Ensuring MOU addresses human resources management and issues.*
- *Institutionalizing professionalism.*
- *Establishing a mechanism to manage temporary personnel.*
- *Utilizing a personnel checklist when assigning or removing personnel from the center (see Sample Checklist on Resource CD).*

Example Staffing

Arizona Counter Terrorism Information Center (ACTIC)
The ACTIC will operate on a 24-hour-a-day/7-day-a-week basis and will function as a multiagency, all-hazard effort staffed by members of the Department of Public Safety and other local, state, and federal agencies.

Rockland County Intelligence Center (RCIC)
RCIC provides services to all law enforcement agencies and is comprised of sworn officers from Rockland County law enforcement agencies. The Intelligence Center officers are assigned specialized "desks." Each desk focuses on a specific type of criminal activity, including burglary/robbery, counter-terrorism, factual data analysis, firearm tracking, identity crimes, organized crime, and street gangs.

Georgia Information Sharing and Analysis Center (GISAC)
GISAC's day-to-day operations, facilities, personnel, finances, and administration are managed by Georgia Bureau of Investigation supervisors. There are a total of 18 personnel assigned.

Statewide Terrorism Intelligence Center (STIC)—Illinois
STIC operates three 24-hour-a-day/7-day-a-week shifts, with a half-hour overlap on each shift for shift-change briefing. Each shift is staffed with one full-time watch officer and four contractual terrorism research specialists (TRS). STIC maintains additional supervisory and operational staff on the day shift. Each employee works a 37.5-hour workweek. Minimum staffing is one supervisor and two TRSs, Monday through Friday, and two TRSs on weekends.

Staffing Model Templates

There are many staffing models in existence; however, most do not focus specifically on law enforcement personnel. Nonetheless, there are some guidelines that leadership can use to help adequately staff a fusion center. During the focus group meetings, the following categories of staffing were recommended. These categories include:

- Collection function—collection management process.
- Analytical services.
- Technical support.
- Communications liaison for dissemination and sharing externally.
- Leadership/command—supporting intelligence-led policing.

This staffing model follows the functions within the intelligence process. Focus group members recommended that the intelligence process dictate the number and level of staffing. It is also important to consider the need for supervisory and management positions, as well as training and information technology support personnel.

Standards for Analysts

In support of the NCISP, the IALEIA published the *Law Enforcement Analytic Standards* booklet, which is included on the accompanying Resource CD. The booklet contains standards regarding education, training, continuing education, professional development, certification, and analytic attributes. It is recommended that centers follow these standards when hiring analysts, preparing individuals for the position of analyst, and/or enhancing an individual's skills and abilities (see Intelligence Services and Products [Guideline 14] for more information).

Available Resources on Fusion Center CD

- Law Enforcement Analytic Standards, http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf
- Personnel Sample Checklist

This Page Is Left Blank Intentionally

Training of Center Personnel

Guideline 12

Ensure personnel are properly trained.

Justification

Training helps personnel maximize the ability to effectively utilize tools in support of center functions. It is recommended that fusion centers adhere to the training objectives outlined in the NCISP. In addition, it is recommended that personnel working within the center meet the core training standards developed by the GIWG and Counter-Terrorism Training Coordination Working Group (CTTWG). Each of the six training classifications identified by the GIWG (intelligence analyst, intelligence supervisor, law enforcement officer, law enforcement executive, intelligence officer/collector, and train-the-trainer) have unique standards. Center personnel should also receive an overview of center operations, policies and procedures, and any unique protocols or communication needs.

Issues for Consideration

When reviewing training, consider:

- *Identifying training needs of center personnel.*
- *Providing specialized training as appropriate.*
- *Providing training in tactical and strategic intelligence.*
- *Seeking accredited or standards-compliant training programs.*
- *Emphasizing analysis and its link to intelligence-led policing.*
- *Developing materials and integrating outreach efforts.*
- *Adhering to other training mandates.*
- *Ensuring that personnel assigned to specific crime desks receive crime-specific training.*
- *Utilizing scenario-based training, simulations, games, tabletops, and field exercises.*

NCISP Training Objectives and Minimum Training Standards

In November 2003, the Criminal Intelligence Training Coordination Strategy (CITCS) Working Group was established to focus on developing a recommended intelligence training coordination strategy. The CITCS recognized that there were voids in existing criminal intelligence training and duplication of effort in terms of training development and delivery. The CITCS met throughout 2004 and finalized their recommendations in June 2004. The CITCS recommendations are contained in the report entitled *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies* and have been endorsed by the GIWG Training/Outreach Committee, the CICC, the CTTWG, and the Global Advisory Committee. The

report is included on the Resource CD. These recommended minimum criminal intelligence training standards were developed for the following training classifications:

- Intelligence analyst
- Intelligence manager
- Law enforcement executive
- General law enforcement officer (basic recruit and in-service)
- Intelligence officer/collector
- Train-the-trainer

These efforts are significant, not only in implementing the tenets of the NCISP but also in building awareness, institutionalizing the importance of criminal intelligence, increasing the value of intelligence personnel, fostering relationships among the law enforcement community, improving the ability to detect and prevent acts of terrorism and other crimes, and creating a safer home for our citizens.

The U.S. Department of Homeland Security (DHS), Office of State and Local Government Coordination and Preparedness is currently developing training in the field of intelligence and information sharing capabilities. Once finalized, this training will be available for widespread utilization by state and local governments, as well as all relevant fusion center participants.[36]

It is also recommended that center staff receive training regarding facility security and operations and information security, as well as the center's policies and procedures.

Available Resources on Fusion Center CD

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov
- HSPD-5, www.whitehouse.gov/news/releases/2003/02/20030228-9.html
- HSPD-8, www.fas.org/irp/offdocs/nspd/hspd-8.html
- Minimum Criminal Intelligence Training Standards, www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf
- IALEIA, www.ialeia.org/
- NW3C, www.nw3c.org
- International Association of Directors of Law Enforcement Standards and Training (IADLEST), www.iadlest.org/

[36] More information about the training opportunities available can be found at the Office of Domestic Preparedness Web site at www.ojp.usdoj.gov/odp/.

Multidisciplinary Awareness and Education

Guideline 13

Provide a multitiered awareness and educational program to implement intelligence-led policing and the development and sharing of information.

Justification

In addition to training center personnel (see Training of Center Personnel [Guideline 12]), it is important to provide general awareness training for all those involved in the intelligence process regardless of whether they are assigned directly to a center. Whether assigned to the center or a customer of the center, it is recommended that all investigative or intelligence personnel, as well as nontraditional collectors of intelligence such as fire, emergency management, and health personnel, receive awareness training. Personnel should be equipped to identify suspicious activities or threats and provide information to fusion center personnel, as appropriate. In addition, policymakers and legislators should understand the center's mission and goals in order to effectively support center efforts, make decisions regarding funding and resource allocation, and respond appropriately during emergencies. Part of this process is developing outreach materials and ensuring that training is ongoing and relevant.

The training objectives and recommended minimum criminal intelligence training standards, developed in support of the NCISP apply to this standard (also see Training of Center Personnel [Guideline 12]). Recommended minimum criminal intelligence training standards have been developed for the following training classifications:

- Intelligence analyst
- Intelligence manager
- Law enforcement executive
- General law enforcement officer (basic recruit and in-service)
- Intelligence officer/collector
- Train-the-trainer

Recommended minimum criminal intelligence training standards for analysts, officers, and collectors include elements regarding how to identify and collect intelligence. In addition, the recommendations for managers and executives offer guidelines and information pertaining to the importance of intelligence, process collecting, analyzing and disseminating intelligence, how to manage and support an intelligence function, and how to develop and adhere to appropriate policies. Many local, state, and private organizations provide awareness-level training; centers should identify appropriate training mechanisms and provide outreach to personnel.

In addition, the general public should be knowledgeable and prepared. This public awareness and education requires a focused and concentrated effort to ensure distribution of important security information.

Issues for Consideration

When reviewing awareness training, consider:

- *Tailoring training based on the needs of individual personnel (i.e., law enforcement officer and executive).*
- *Identifying what elements intelligence personnel need regarding center operations.*
- *Developing materials and integrating outreach efforts.*
- *Communicating with all agencies serviced by the center to ensure appropriate training.*
- *Prioritizing intelligence function to address threats posed in specific fusion center jurisdictions.*
- *Integrating intelligence-led policing to support customer needs, define tasks, and prioritize functions.*

Available Resources on Fusion Center CD

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov
- Minimum Criminal Intelligence Training Standards, www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf
- HSAC Homeland Security Intelligence and Information Fusion Report

Intelligence Services and Products

Guideline 14

Offer a variety of intelligence services and products to customers.

Justification

The majority of the initiatives reviewed during the focus group process provide 24-hour-a-day/7-day-a-week operations and act as a clearinghouse for information and/or intelligence sharing. The intelligence process acts as the framework. Personnel provide analytical services, such as crime-pattern analysis, association analysis, telephone-toll analysis, flowcharting, financial analysis, and strategic analysis.

In addition, the initiatives provide an array of intelligence products, such as intelligence reports, briefs, threat assessments, charts, graphs, and mapping. It is also important that center personnel, especially analysts, be familiar with computer applications that have information storage capabilities which allow the user to sort, query, and filter information; applications utilized for presenting information; and applications used for linking and flowcharting.

Some initiatives have compartmentalized their operation by creating divisions, such as investigations, intelligence, and administration. This structure may assist in identifying and assigning responsibilities, as well as holding personnel accountable. It is important to know who the program's customers are and what types of services and products will meet their needs.

Issues for Consideration

It is recommended that law enforcement intelligence programs produce both strategic and tactical products to support the mission and priorities of the center. A major purpose of intelligence analysis is for management decision making. Consider providing the following services and products:

- *Investigative and tactical response*
- *Proactive strategic analysis*
- *Intelligence support for investigations*
- *Visual investigative analysis*
- *Alert and notification*
- *Deconfliction*
- *Target identification*
- *Critical infrastructure analysis*
- *Criminal backgrounds and profiles*
- *Case correlation*
- *Crime-pattern analysis*
- *Association, link, and network analysis*
- *Telephone-toll analysis*
- *Flowcharting*
- *Financial analysis*
- *Intelligence reports and briefings*
- *Threat assessments*

In addition, it is recommended that centers prioritize their intelligence function based on specific threats in their jurisdictions/regions and integrate intelligence-led policing to support customer needs, define tasks, and prioritize functions.

Standards for Analytical Products

The NCISP recommends that the agency chief executive officer and the manager of intelligence functions should "support the development of sound, professional analytic products (intelligence)." One way to accomplish this is to recommend that products meet substantive criteria. In IALEIA's *Law Enforcement Analytic Standards* booklet, standards for analysis are provided that correspond to the intelligence process. The standards focus on the following components:

- Planning
- Direction
- Collection
- Legal constraints
- Evaluation
- Collation
- Analytic accuracy
- Computerized analysis
- Analytic product content
- Analytic outcomes
- Dissemination plan
- Analytic report
- Analytic product format
- Analytic testimony
- Data source attribution
- Analytic feedback
- Analytic production evaluation

It is recommended that analysts or individuals fulfilling the analytic function adhere to the standards outlined in the booklet. A copy of the booklet is included on the Resource CD.

Infrastructure Assessment and Resources

A significant role for any intelligence fusion center that is concerned with homeland security is the tracking of critical infrastructure and assessing its likelihood to be the target of a terrorist attack. The center will need to catalog all critical infrastructures in its area of responsibility, develop a methodology to track intelligence relating to threats against those facilities, maintain and share with partners a list of special events that may pose a threat (e.g., high visibility, large crowds), and develop a mechanism to update this information on a regular basis.

Additionally, the center may be tasked with developing assessments of the vulnerabilities and security protocols for critical facilities in their jurisdiction. This may range from simply maintaining the assessments completed by others to actually participating in the on-site assessments. Either way, it is important that the center receive the information for fusion into its intelligence databases. The fusion center may consider working with the area JTTF, ATAC, and/or DHS as well as other state and local authorities to design and implement protective measures that mitigate identified vulnerabilities. Included in the resource documents is a section from the Florida Department of Law Enforcement (FDLE) Terrorism Protection Manual that covers critical infrastructure assessments.

The DHS Information Analysis and Infrastructure Protection (IAIP) Directorate helps deter, prevent, and mitigate acts of terrorism by assessing vulnerabilities. More information regarding IAIP's programs can be viewed at www.dhs.gov.

Available Resources on Fusion Center CD

- DHS National Response Plan, December 2004
- Terrorism Protection Manual, FDLE, February 28, 2003

This Page Is Left Blank Intentionally

Policies and Procedures

Guideline 15

Develop, publish, and adhere to a policies and procedures manual.

Justification

The focus group recommended that fusion centers utilize formalized policies and procedures. A comprehensive policies and procedures manual offers a number of advantages.[37] It demonstrates that the center has provided direction of actions of its employees and that personnel followed approved procedures in carrying out their duties. In addition, policies and procedures indicate that the governing body has been proactive in planning, instead of reactive or waiting until an incident occurs to write policy. The policies and procedures manual is the foundation for communications within the center and among personnel. By developing, publishing, and adhering to a policies and procedures manual, the expectations of personnel are outlined creating consistency and accountability while reducing liability and enhancing the overall professionalism of the center. A policies and procedures manual also serves as a central repository for all center directives. It is important for personnel to easily locate the center's most recent procedures.

Issues for Consideration

When designing a policies and procedures manual, consider the following guidelines:[38]

- *Outlining the roles and responsibilities of all parties involved.*
- *Including language that information should only be used for criminal investigations.*
- *Including the center's mission, goals, objectives, policies, procedures, rules, and regulations.*
- *Tailoring the manual to meet the needs of the center.*
- *Ensuring personnel have easy access to the manual. Providing employees a copy of the manual and/or providing an online manual.*
- *Using a standardized format to allow for easy reading, filing, retrieving, and correcting.*
- *Implementing an annual review of center directives and purging or revising outdated policies and procedures.*
- *Establishing a contractor's code of conduct.*
- *Citing of the policy and procedures manual in the MOU (Guideline 5).*

[37] Michael Carpenter, M.A., M.A.T., "Put It in Writing: The Police Policy Manual", *FBI Law Enforcement Bulletin*, Vol. 69, No. 10, October 2000.
[38] Ibid.

Suggested Policies and Procedures

It is also important to identify existing guidelines, statutes, policies, and procedures that affect center operations and ensure adherence to regulations, such as 28 CFR Part 23. Personnel should be trained on and understand all center processes and policies and procedures and adhere to them at all times. Areas that may require policies and procedures include:

- Intelligence process (refer to NCISP [Guideline 1]).
- Intelligence collection requirements.
- Security for data, facility, personnel, and systems (refer to Security Guideline; Facility, Location, and Physical Infrastructure Guideline; and Human Resources Guideline for more information).
- Communications (refer to Interconnectivity [Guideline 7] for more information).
- Privacy (refer to Privacy [Guideline 8] for more information).
- Accountability and review.
- Sanctions and violations of policies and procedures.

28 CFR Part 23

Agencies that use federal funds to set up or maintain a criminal intelligence database (and share information between jurisdictions) may need to comply with the regulations of 28 CFR Part 23. The regulations require agencies to have policies and procedures in place regarding intelligence operations. The specifics of the policies are left to the individual agencies. A copy of this regulation is included on the accompanying Resource CD. Additional information may also be found at www.iir.com/28cfr.

In addition to the regulations of 28 CFR Part 23, the NCISP also recognizes the following documents and guidelines for creating and implementing a policies and procedures manual: the *Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines* and the *Justice Information Privacy Guideline*.

Available Resources on Fusion Center CD

- 28 CFR Part 23, www.iir.com/28cfr/Overview.htm
- Evaluation Checklists for Intelligence Units
- IACP Criminal Intelligence Model Policy
- Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines, http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf
- *Justice Information Privacy Guideline,* www.ncja.org/pdf/privacyguideline.pdf

Center Performance Measurement and Evaluation

Guideline 16

Define expectations, measure performance, and determine effectiveness.

Justification

It is important to have a process that systematically reviews performance. Performance measurement review is critically important to the health of an organization. The review must accurately reflect existing performance and operate to initiate improvement. Reviewing an entity's objectives is required to ensure integrity of the measurement process and to justify continued investment in the organization and/or project. Only an effective and verifiable performance measurement-and-review process can address these concerns. The performance measures addressed under this standard refer to the center's performance, not an individual's performance or expectations. Personnel issues are addressed under the Human Resources (Guideline 11).

Due to the unique structure of fusion centers, traditional law enforcement measures may not adequately gauge center performance. Performance measures should be designed based on the center's core mission, goals, and objectives and should reflect services generated from all areas of the center. It is also important to note that often performance measures and funding are related. Management should consider this relationship when developing measures and reviewing/submitting funding requests.

In addition to measuring performance, centers may consider developing an evaluation process. It is important to distinguish between performance measurement and evaluation. Performance measures assess center services and accomplishment of mission. Evaluation, on the other hand, reflects value judgments regarding the adequacy, appropriateness, and success of a particular service or activity.[39] In other words, performance measures focus on the "what" while evaluation focuses on the "why."

Issues for Consideration

When establishing performance measures and evaluating effectiveness, consider:

- *Defining the expected performance.*
- *Developing outputs and outcomes that measure the expected performance.*
- *Coordinating the development and review of measures and performance with participating agencies.*
- *Developing meaningful relevant and quantifiable measures.*
- *Creating measures that are based on valid and reliable data.*

[39] Charles R. McClure, *Performance Measures*, School of Information Studies, Syracuse University, 1996.

  - *Validity—ask the question: "Does the information actually represent what we believe it represents?"*
  - *Reliability—ask the question: "Is the source of the information consistent and dependable?"*
- *Creating both internal and external measures—internal measures pertain to administrative purposes.*
- *Establishing reasonable standards and targets.*
- *Leveraging which systems and databases statistically capture data.*
- *Utilizing automation to capture, store, and report performance.*
- *Reporting and reviewing on performance regularly (i.e., board or managers' meetings) and adjusting operations, as appropriate.*
- *Publicizing performance to the public, policymakers, and customers.*
- *Creating accountability and deterring the consequences for not meeting targets.*
- *Surveying customers.*
- *Developing a strategic plan to guide operations.*

Elements of Good Performance Measures

Generally accepted guidelines for developing performance measures include:

- Using standard terms and definitions.
- Gauging progress towards agency goals and benchmarks or other high-level outcomes.
- Focusing on key issues.
- Having reasonable targets.
- Basing on accurate and reliable data.
- Being easily understood and measuring performance in a single area.
- Being timely.
- Limiting subjectivity—being objective.

Using Performance Measures

Once performance measures are developed, baseline data will need to be obtained during the first year of operation. Baseline data will assist managers in determining the standards for future years. Measures should reflect center goals and be quantifiable. Standards should be challenging to achieve but also realistic. Management should review performance regularly and inform center personnel of progress. By keeping employees informed and involving them in the performance-measure process, they will be motivated to work collectivity to reach targeted goals. Performance measures can be tied to funding and resource requests and have a significant impact on support and future endeavors.

Available Resources on Fusion Center CD

- Office of Management and Budget, www.omb.gov
- Performance Measurement Tools for Justice Information Technology Project, www.cslj.net/PerformanceMeasure/links.htm
- University of California, San Diego—*Guide to Performance Management*, www-hr.ucsd.edu/~staffeducation/guide/standard.html#How

This Page Is Left Blank Intentionally

Funding

Guideline 17

Establish and maintain the center based on funding availability and sustainability.

Justification

Funding is a critical element in establishing fusion centers. Funding directly impacts a fusion center's longevity and ability to effectively and efficiently operate. Often new initiatives receive start-up funds through government programs and/or grants. This "seed" money is an excellent means for beginning new projects or programs. Unfortunately, some efforts end because initial funding has been spent and no additional funding was identified or obtained to continue the project. For the long term, it is essential that centers take responsibility for funding to ensure sustainability. It is recommended that center management identify the needs of the center and identify available funding sources, to include local, state, federal, and nongovernmental sources.

Issues for Consideration

When reviewing funding needs and sources, consider:

- *Basing funding on center priorities.*
- *Leveraging existing resources/funding from participating entities.*
- *Ensuring resource commitment of participating entities is addressed via MOU.*
- *Identifying supplemental funding sources (i.e., seized assets/forfeitures, local and state government appropriations, state and federal grants, and private sources).*
- *Establishing operational budget.*
- *Adhering to reporting requirements (i.e., annual report).*

Center Expenses

In order to effectively operate a fusion center, a number of cost elements must be identified and addressed in a budget. Some of these expenses can be shared among participating agencies. The following is a sample list of budgetary expenses that will require funding:

- Salary
- Vehicles
- Equipment
- Supplies/commodities
- Facility
- Furnishing
- Information technology support
- Communication equipment
- Training
- Travel
- Contractual (copier, delivery)
- Printing

Available Resources on Fusion Center CD

- The U.S. Government's Official Web Portal, www.firstgov.gov
- Summary of Funding Resources

Next Steps

Fusion centers represent a capability for law enforcement, public safety, and private entities to securely develop and share information and intelligence in an innovative, effective, and efficient manner. Many of the issues impacting fusion centers have been addressed in this report, specifically those affecting the intelligence function of fusion centers. Undeniably, as centers are established, additional issues will arise, best practices will emerge, and future needs will be identified. This document is not meant to be all inclusive; instead, the recommendations contained herein are the foundation for a much larger and complex enterprise. As this process continues, the focus group members remain committed to sharing information about fusion center development, operations, and services with all levels of law enforcement. Further developments and materials will be provided on the OJP Web site at www.it.ojp.gov.

The focus group members identified a number of issues for consideration and next steps. Specifically, during the January 2005 meeting of the focus group, strategies were discussed to integrate public safety, emergency management, and private partners into the fusion center concept. With this expansion in scope, additional guidelines, model policies, and resources will be established, requiring modification of the current focus group's mission and membership to include public safety and private entities.

The focus group also discussed the need to disseminate this and future reports or materials to key organizations such as the International Association of Chiefs of Police, National Sheriffs' Association, Major Cities Chiefs Association, and Homeland Security Advisors, as well as all local and state government agencies and private entities. It is critical that this information be provided to agencies quickly. Furthermore, it was suggested that articles be drafted and submitted to law enforcement, criminal justice, and other relevant publications to further disseminate the guidelines and resource materials.

As recommended in this report, fusion centers should be established in all states to allow for the maximum capability of intelligence and information exchange. Although guidelines are not meant to be mandatory, discussion ensued among the focus group members to urge funding agencies to grant funds to entities that adhere to these minimum guidelines.

Moving from a reactive response approach to a proactive and preventive approach will improve law enforcement's ability to detect and prevent crime and public safety personnel's capability to respond to emergencies. The fusion center concept is an opportunity to bring together critical resources and produce meaningful information and intelligence for dissemination to the right people at the right times for the right reasons. Through a collective, collaborative implementation process, the center, the personnel, and the citizens the center serves will benefit.

This Page Is Left Blank Intentionally

Appendix A
Focus Group Participants and Acknowledgements

Focus Group Participants

Peter A. Modafferi, Chief (Chairman)
Rockland County, New York, District Attorney's Office

Norm Beasley, Lieutenant Colonel
Arizona Counter Terrorism Information Center

Kenneth A. Bouche, Colonel
Illinois State Police

Roger Bragdon, Chief
Spokane, Washington, Police Department

David Carter, Ph.D.
Michigan State University

Stephen Clark
Georgia Emergency Management Agency

Daniel Cooney, Captain
Upstate New York Regional Intelligence Center

C. Patrick Duecy
Homeland Solutions, LLC

John T. Elliff
Federal Bureau of Investigation

Dennis Ellis, Lieutenant
Indiana State Police

William Fennell, Program Manager
U.S. Drug Enforcement Administration

Max Fratoddi
Counterdrug Intelligence Executive Secretariat

Bob Hardin, Inspector
Georgia Bureau of Investigation

Chris Holmes, Deputy Program Manager
ManTech Information Systems and Technology
U.S. Department of Homeland Security

Cliff Karchmer, Director
Police Executive Research Forum

Clark Kimerer, Deputy Chief
Seattle, Washington, Police Department

Mark Marshall, Chief
Smithfield Police Department

Jerry Marynik, Administrator
State Terrorism Threat Assessment Center

Mary Meyer, Officer
Minnesota Department of Public Safety

Doug Poole, Acting Chief
U.S. Drug Enforcement Administration

Russ Porter, Chief
Iowa Department of Public Safety

Don Robertson
Georgia Bureau of Investigation

Richard A. Russell
U.S. Department of Homeland Security

Kurt Schmid, Senior Advisor
Office of National Drug Control Policy

Clark Smith, Senior Information Technology Specialist
U.S. Department of Justice

Mike Snyders, Lieutenant Colonel
Illinois State Police

Nicholas Theodos, Major
New Jersey State Police

Mark Zadra, Chief
Florida Department of Law Enforcement

Acknowledgements

Daron Borst, Supervisory Special Agent
Federal Bureau of Investigation

Tom Brozycki, Investigator
Upstate New York Regional Intelligence Center

Hyuk Byun, Program Executive, Communications and Information Technology
National Institute of Justice

David Clopton, Ph.D.
National Institute of Justice

John Cohen, Senior Advisor
Executive Office of Public Safety, Massachusetts

Jeffrey Gaynor
U.S. Department of Homeland Security

Matthew Jack, Supervisory Special Agent
U.S. Department of Homeland Security

Bart Johnson, Lieutenant Colonel
New York State Police

Harri j. Kramer
U.S. Department of Homeland Security

George Marenic
U.S. Department of Homeland Security

J. Patrick McCreary, Associate Deputy Director
Bureau of Justice Assistance

Mike Miron
U.S. Department of Homeland Security

John Morgan, Ph.D., Assistant Director for Science and Technology
National Institute of Justice

Richard Randall, Sheriff
Kendall County, Illinois, Sheriff's Office

Jeffrey Sands, Special Advisor
U.S. Department of Homeland Security

Kelly Tapp, Communications Manager
U.S. Department of Justice

Karen Waterman
U.S. Department of Homeland Security

Colleen Wilson
U.S. Department of Homeland Security

This Page Is Left Blank Intentionally

Appendix B
Fusion Center CD Resources

Fusion Center CD Resources

Guideline 1 – The NCISP and the Intelligence Process

- 10 Simple Steps to help your agency become a part of the *National Criminal Intelligence Sharing Plan*
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*
- *National Criminal Intelligence Sharing Plan* report

Guideline 2 – Mission Statement and Goals

- *The Community Policing Consortium – Staircase to Strategic Planning: Mission,* www.communitypolicing.org/mission.html

Guideline 3 – Governance

- Bylaws Sample Template
- Board Guidelines, www.mapnp.org/library/boards/boards.htm
- Global Justice Information Sharing Initiative Advisory Committee bylaws, http://it.ojp.gov/documents/GACBylaws.pdf
- Parliamentary Procedures, www.rulesonline.com

Guideline 4 – Collaboration

- Community Collaboration, www.communitycollaboration.net

Guideline 5 – Memorandum of Understanding (MOU)

- 28 CFR Part 23 Sample MOU
- Arizona Counter Terrorism Information Center MOU
- Canada Department of Defense (DOD) MOU Guidelines
- Joint Terrorism Task Force MOU
- MOU Sample Template
- Rockland County Intelligence Center MOU
- Upstate New York Regional Intelligence Center MOU

Guideline 6 – Database Resources

- El Paso Intelligence Center (EPIC), www.usdoj.gov/dea/programs/epic.htm
- FBI's LEO Program, www.fbi.gov/hq/cjisd/leo.htm
- Financial Crimes Enforcement Network (FinCEN), www.fincen.gov
- High Intensity Drug Trafficking Areas (HIDTA), www.whitehousedrugpolicy.gov/hidta/index.html
- Homeland Security Information Network (HSIN), www.dhs.gov/dhspublic/display?content=3350
- International Association of Crime Analysts (IACA), www.iaca.net
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org
- International Criminal Police Organization (INTERPOL), www.usdoj.gov/usncb/
- Law Enforcement Intelligence Unit (LEIU), www.leiu-homepage.org/main.cgi
- National Crime Information Center (NCIC), www.fbi.gov/hq/cjisd/ncic.htm

- National Drug Intelligence Center (NDIC), www.usdoj.gov/ndic
- National White Collar Crime Center (NW3C), www.nw3c.org and www.training.nw3c.org
- NLETS – The International Justice and Public Safety Information Sharing Network, http://64.132.171.113/index.asp
- RISS Automated Trusted Information Exchange (ATIX), www.rissinfo.com/rissatix.htm
- RISSNET™, www.rissinfo.com

Guideline 7 – Interconnectivity

- *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*, http://it.ojp.gov/documents/200409_Global_Infrastructure_Report.pdf
- Model Intelligence Database Policy
- *A Critical Look at Centralized and Distributed Strategies for Large-Scale Justice Information Sharing Systems* (a white paper prepared by the IJIS Institute)
- Global Justice XML Data Model (Global JXDM), www.it.ojp.gov/gjxdm

Guideline 8 – Privacy

- Audit Checklist (LEIU), www.it.ojp.gov/documents/LEIU_audit_checklist.pdf
- *Global Privacy and Information Quality Policy Development for the Justice Decision Maker*, http://it.ojp.gov/documents/200411_global_privacy_document.pdf
- National Criminal Justice Association—Justice Information Privacy Guideline, www.ncja.org/pdf/privacyguideline.pdf
- Privacy Policy Sample Template

Standard 9 – Security

- *Applying Security Practices to Justice Information Sharing*, http://it.ojp.gov/documents/asp/introduction/index.htm
- National Institute of Standards and Technology (NIST) template and example policies, http://csrc.nist.gov/fasp
- *Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs,* U.S. Department of Homeland Security, May 2005

Guideline 10 – Facility, Location, and Physical Infrastructure

- IACP Police Facility Planning Guidelines, www.iacp.org/documents/pdfs/Publications/ACF2F3D%2Epdf
- Executive Orders 12068, 12958, and 13292 regarding classified information
- FBI Security Clearances and Frequently Asked Questions

Guideline 11 – Human Resources

- Law Enforcement Analytic Standards, http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf
- Personnel Sample Checklist

Guidelines 12 and 13 – Training of Center Personnel/Multidisciplinary Awareness and Education

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov
- HSPD-5, www.whitehouse.gov/news/releases/2003/02/20030228-9.html
- HSPD-8, www.fas.org/irp/offdocs/nspd/hspd-8.html
- Minimum Criminal Intelligence Training Standards, www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org/
- NW3C, www.nw3c.org/
- International Association of Directors of Law Enforcement Standards and Training (IADLEST), www.iadlest.org/
- HSAC Homeland Security Intelligence and Information Fusion Report

Guideline 14 – Intelligence Services and Products

- DHS National Response Plan, December 2004
- Terrorism Protection Manual, FDLE, February 28, 2003

Guideline 15 – Policies and Procedures

- 28 CFR Part 23, www.iir.com/28cfr/Overview.htm
- Evaluation Checklists for Intelligence Units
- IACP Criminal Intelligence Model Policy
- Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines, http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf
- *Justice Information Privacy Guideline*, www.ncja.org/pdf/privacyguideline.pdf

Guideline 16 – Center Performance Measurement and Evaluation

- Office of Management and Budget, www.omb.gov
- Performance Measurement Tools for Justice Information Technology Project, www.cslj.net/PerformanceMeasure/links.htm
- University of California, San Diego—*Guide to Performance Management*, www-hr.ucsd.edu/~staffeducation/guide/standard.html#How

Guideline 17 – Funding

- The U.S. Government's Official Web Portal, www.firstgov.gov
- Summary of Funding Resources

Organization Links

- CopNet, www.copnet.org
- Defense Information Systems Agency, www.disa.mil
- FBI Terrorism Information, www.fbi.gov/terrorinfo/counterterrorism/waronterrorhome.htm
- International Association of Crime Analysts (IACA), www.iaca.net
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org
- Integrated Justice Information Systems Institute, www.ijis.org

- National Association of Counties, www.naco.org
- National Association of State Chief Information Officers, www.nascio.org
- National Governors Association project on justice information sharing, www.nga.org
- Office of Management and Budget, www.omb.gov
- Office of Justice Programs of the U.S. Department of Justice, www.it.ojp.gov
- Regional Information Sharing Systems®, www.rissinfo.com
- SEARCH, The National Consortium for Justice Information and Statistics, www.search.org
- Terrorism Research Center, www.terrorism.com
- U.S. Department of Defense News, www.defendamerica.mil
- U.S. Department of Homeland Security, www.dhs.gov
- U.S. Department of Justice, www.justice.gov
- U.S. Department of State, www.state.gov/s/ct

This Page Is Left Blank Intentionally

Appendix C
HSAC Homeland Security Intelligence and Information Fusion Report
(April 28, 2005)

This Page Is Left Blank Intentionally

U.S. DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY ADVISORY COUNCIL

INTELLIGENCE AND INFORMATION SHARING INITIATIVE:

HOMELAND SECURITY INTELLIGENCE & INFORMATION FUSION

APRIL 28, 2005

JOSEPH J. GRANO, JR.
CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

WILLIAM H. WEBSTER
VICE CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

DANIEL J. OSTERGAARD
EXECUTIVE DIRECTOR
HOMELAND SECURITY ADVISORY COUNCIL

MITT ROMNEY
CHAIRMAN
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

JOHN COHEN
EXECUTIVE DIRECTOR
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

MICHAEL J. MIRON
DIRECTOR
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

Background

Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about who the enemies are,[40] where and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use. This information should serve as a guide for efforts to:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and
- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism–related information. It can come through the efforts of the intelligence community; Federal, State, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, healthcare, general government), and the private sector (e.g., transportation, healthcare, financial, Internet/information technology).

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 most State and local law enforcement entities. The attacks of September 11, 2001, however, taught us 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. Important intelligence that may forewarn of a future attack may be derived from information collected by State, tribal, and local government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.

The President and the U.S. Congress have directed that an information sharing environment (ISE) be created in the next two years to facilitate information sharing and collaboration activities within the Federal Government (horizontally) and between Federal, State, tribal, local, and private-sector entities (vertically). The concept of intelligence/information fusion has emerged as the fundamental process (or processes) to facilitate the sharing of homeland security-related information and intelligence at a national level, and, therefore, has become a guiding principle in defining the ISE.

[40] Including their capabilities, intentions, strengths, weaknesses.

Homeland Security Intelligence/Information Fusion

Homeland security intelligence/information fusion is the overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private-sector authorities. It is more than the 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. Intelligence fusion is a clearly defined, ongoing process that involves the delineation of roles and responsibilities; the creation of requirements; and the collection, blending, analysis, timely dissemination, and reevaluation of critical data, information, and intelligence derived from the following:

- Autonomous intelligence and information management systems (technical and operational) established to support the core missions of individual Federal, State, local, tribal, and government entities;
- General public; and
- Private-sector entities.

The fusion process is a key part of our nation's homeland security efforts. This process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. Simultaneously, it supports efforts to address immediate and/or emerging, threat-related circumstances and events. Although the collection, analysis, and dissemination of terrorism-related intelligence is not the sole goal of the fusion process, one of the principal outcomes should be the identification of terrorism-related leads—that is, any nexus between crime-related and other information collected by State, local, tribal, and private entities and a terrorist organization and/or attack. The fusion process does not replace or replicate mission-specific intelligence and information management processes and systems. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may be indicative of an emerging threat condition. Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to State, tribal and local entities is that it will support ongoing efforts to address nonterrorism related issues by:

- Allowing State and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends;
- Supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and
- Improving the delivery of emergency and nonemergency services.

Effective intelligence/information fusion requires the following:

- The use of common terminology, definitions, and lexicon by all stakeholders;
- Up-to-date awareness and understanding of the global and domestic threat environment;
- A clear understanding of the links between terrorism-related intelligence and nonterrorism-related information (e.g., flight school training, drug trafficking) so as to identify those activities that are precursors or indicators of an emerging threat;
- Clearly defined intelligence and information requirements with the Federal intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts;
- Identifying critical information repositories[41] and establishing the processes, protocols, procedures, and technical capabilities to extract information and/or intelligence from those repositories;
- Reliance on existing information pathways and analytic processes as possible;
- All-hazards and all-crimes approach to defining information collection, analysis, and dissemination;
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process;
- Understanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide and/or local fusion efforts);
- Capacity to convert information into operational intelligence;
- Extensive and continuous interaction with the private sector and with the public at large;
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories at all levels of classification as necessary;
- Extensive participation of subject-matter experts (SMEs) in the analytical process; and

[41] These repositories are not limited to those maintained by law enforcement entities. For example, critical information may be contained in systems supporting medical examiners (unattended death), public health entities, emergency rooms (information similar to the Drug Abuse Warning Network program), environmental regulatory inspectors, transportation entities, housing inspectors, health inspectors, building code inspectors, etc.

- Capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

Participants in the Fusion Process

To some degree, the fusion process involves every level and sector (discipline) of government, the private-sector, and the public. The level of involvement from these participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process because of the relationship between crime and because, in many cases, law enforcement authorities are best-suited to coordinate statewide and local fusion efforts. Minimally, the fusion process should be organized and coordinated on a statewide level and each State should establish and maintain an analytic center to facilitate the fusion process. Each major urban area (as defined by the Urban Area Security Initiative [UASI] program) may want to establish a similar capacity ensuring it is interlinked with the fusion process established by the State. Other localities, tribal governments, and even private-sector entities should develop a process to interlink and participate in these statewide (or UASI) fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activities or circumstances.

Efforts should be organized and managed on a geographic basis and scalable so adjustments can be made based on changes in the operating and/or threat environment. While national standards and guidelines should guide the institutionalization of the process, the actual technological infrastructure and operational protocols used by individual jurisdictions should be based on the management structure, specific needs, and capabilities of each individual jurisdiction.

Stages of the Fusion Process

Fusion is cyclical process that includes the following stages and activities:

- **Management/Governance**
  - Define a management structure (e.g., who is in charge, what entity will manage and coordinate daily activities).
  - Identify core (permanent) and ad hoc stakeholders.
  - Design a governance structure advisory committee (multidisciplinary and multilevel of government).
  - Define goals and objectives.
  - Develop a process to define information and intelligence collection requirements.
  - Develop the process and necessary memorandums of understanding to communicate requirements.

- **Planning and Requirements Development**
  - Conduct (and update frequently) a comprehensive and compatible risk assessment (threat, vulnerability, and consequence).
  - Identify patterns and trends reflective of emerging threats.
  - Define collection requirements based on results of risk assessments.
  - Identify the circumstances or events (e.g., crime, public health) that represent indicators and/or precursors of threats.
  - Identify the sources and/or repositories of data and information regarding indicators and precursors.
  - Identify the existing capacity to collect key information from existing sources.
  - Identify collection gaps and mitigate.
  - Define public education, and other activities necessary to enhance situational awareness by the public.
  - Develop training for front line law enforcement and other personnel so that they can better identify suspicious activities that may represent planning and/or operational activity by terrorist group.
  - Ensure a mechanism exists to support reporting of collected information (e.g., 9-1-1, tipline, Internet, connectivity to key information systems).
  - Identify regulatory, statutory, privacy, and/or other issues that impede collection and sharing of information.
  - Develop (in partnership with private-sector officials) detailed knowledge of vulnerabilities and consequence in the private sector to possible terrorist attacks to assess the likelihood of attack, the likely methods of attack, the likely equipment and substances used to carry out such an attack, and identify planning activities.
- **Collection**
  - Communicate collection requirements to relevant State, tribal, local, and private-sector entities.
  - Implement situational awareness activities (e.g., training, public education).
  - Mitigate impediments to collection.
  - Compile classified and unclassified data, information and intelligence generated by people and organizations.

- Serve as the 24/7/365 initial point of contact for information provided by the U.S. Department of Homeland Security, Department of Defense, Department of Justice, Federal Bureau of Investigation, and other Federal entities (via telephone calls, Homeland Security Information Network/Joint Regional Information Exchange System, LEO, e-mail bulletins, VTC, fax) for the receipt of the following:
  - Immediate threat-specific information (classified and unclassified)
  - Long-term threat information (classified and unclassified)
  - Tactics and methods used by terrorists (classified and unclassified)
- Integrate with other reporting systems (e.g., 9-1-1, 3-1-1), and establish and maintain further, easy-to-use capability for the public reporting of suspicious activity in conjunction with the Joint Terrorism Task Force (e.g., internet, toll-free tipline).
- Establish a process to identify and track reports of suspicious circumstances (e.g., pre-operational surveillance, acquisition of items used in an attack).

- **Analysis**
  - Blend data, information, and intelligence received from multiple sources.
  - Reconcile, deconflict data, and validate as to credibility of data, information and intelligence received from collection sources.
  - Evaluate and analyze data and information using SMEs.
  - Identify and prioritize the risks faced by the jurisdiction (e.g., State, local).
  - Produce value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and consequence management programs.
  - Identify specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages.

- **Dissemination, Tasking, and Archiving**
  - Identify those entities and people (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management (public and private) efforts.
  - Provide relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sector).
  - Archive all data, information, and intelligence to support future efforts.

- Support the development of performance-based prevention, response, and consequence management measures.
- Establish the capacity to track performance metrics associated with prevention, response, and consequence management efforts.
- Provide feedback to information collectors.

- **Reevaluation**
  - Track the achievement of prevention, response, and consequence management program performance metrics so as to evaluate impact on the risk environment.
  - Update threat, vulnerability, and consequence assessments so as to update the risk environment.
  - Assess effectiveness of national (i.e., Federal, State, tribal, and local) intelligence and information collection requirements process.

- **Modification of Requirements**
  - Modify collection requirements as necessary.
  - Communicate modifications in a timely manner.

Intelligence and Information Sharing Working Group Members

Chair, Governor Mitt Romney (Homeland Security Advisory Council [HSAC])
Chuck Canterbury (HSAC)
Frank Cilluffo (HSAC)
Major General Bruce Lawlor (Retired) (HSAC)
Mayor Patrick McCrory (HSAC)
Lydia Thomas (HSAC)
Mayor Karen Anderson (State and Local Senior Advisory Committee [SLSAC])
James Dunlap (SLSAC)
Don Knabe (SLSAC)
Peggy Merriss (SLSAC)
Karen Miller (SLSAC)
Mayor Donald Plusquellic (SLSAC)
Michael Carona (Emergency Response Senior Advisory Committee [ERSAC])
Frank Cruthers (ERSAC)
Ellen Gordon (ERSAC)
Phillip Keith (ERSAC)
Paul Maniscalco (ERSAC)
Dr. Allan Zenowitz (Academe, Policy and Research Senior Advisory Committee)
George Vradenburg (Private Sector Senior Advisory Committee)
John Cohen (Office of the Governor, Massachusetts)
Cindy Gillespie (Office of the Governor, Massachusetts)

Fusion Group Subject-Matter Experts

Kenneth Bouche, Colonel, State Police, Illinois
Dan Cooney, Captain, State Police, New York
George Foresman, Homeland Security Advisor, Virginia
Bart Johnson, Lieutenant Colonel, State Police, New York
Fred LaMontagne, Fire Chief, Maine
Pete Modafferi, Chief of Detectives, Rockland County, New York
Steve McGraw, Homeland Security Advisor, Texas
Jim Mcmahon, Homeland Security Advisor, New York
Tom O'Reilly, Office of the Attorney General, New Jersey
Russ Porter, Assistant Director, Department of Public Safety, Iowa
Mark Zadra, Chief of Investigations, Office of Statewide Intelligence, Florida

Homeland Security Advisory Council Staff

Dan Ostergaard, Executive Director, Homeland Security Advisory Council
Rich Davis, Director, Academe and Policy Research Senior Advisory Committee
Jeff Gaynor, Director, Emergency Response Senior Advisory Committee
Katie Knapp, Special Assistant to the Homeland Security Advisory Council
Mike Miron, Director, State and Local Officials Senior Advisory Committee
Candace Stoltz, Director, Private Sector Senior Advisory Committee

This Page Is Left Blank Intentionally

Appendix D
Fusion Center Report Glossary

This Page Is Left Blank Intentionally

Fusion Center Report Glossary

28 CFR Part 23—A guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. (Criminal Intelligence Glossary, November 2004)

Administrative Analysis—The provision of economic, geographic, or social information to administrators. (Gottlieb, Singh, and Arenberg, 1995, p. 13) The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions. (Criminal Intelligence Glossary, November 2004)

Advanced Authentication—Definitively identifying users before they access an organization's network is a key component in protecting information resources. Start by choosing an authentication system with encrypted password protocols. Before choosing an advanced authentication system, it is imperative that data owners evaluate user access, hardware, and other requirements. (Criminal Intelligence Glossary, November 2004)

Analysis—The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. (Peterson, 1994, p. 269) That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment. (Criminal Intelligence Glossary, November 2004)

Association/Link/Network Analysis—Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best. (Law Enforcement Analytic Standards, November 2004) The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix. (Criminal Intelligence Glossary, November 2004)

Audit Trails—The use of audit procedures (e.g., tracking who is accessing the data or what data was accessed) combined with analysis of audit logs and follow-up for unauthorized or anomalous activity is essential for long-term system security and privacy. (Criminal Intelligence Glossary, November 2004)

Classified Information/Intelligence—A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure certain information be maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities. (Criminal Intelligence Glossary, November 2004)

> **Top Secret Classification**—Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. (Executive Order 12958, March 25, 2003).

Secret Classification—Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (Executive Order 12958, March 25, 2003).

Confidential Classification—Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (Executive Order 12958, March 25, 2003).

Collation (of Information)—The process whereby information is assembled together and compared critically. (Law Enforcement Analytic Standards, November 2004) A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval. (Criminal Intelligence Glossary, November 2004)

Collection (of Information)—The directed, focused gathering of information from all available sources. (INTERPOL, 1996, p. 9) The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal. (Criminal Intelligence Glossary, November 2004)

Commodity Flow Analysis—Graphic depictions and descriptions of transactions, shipments, and distribution of contraband goods and money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities. (Criminal Intelligence Glossary, November 2004)

Concept of Operations (CONOPS)—A statement outlining how an operation or organization will achieve its mission and goals. The concept is designed to give an overall picture of the operation.

Continuity of Operations Plan—A plan that specifies the activities of individual departments and agencies and their subcompartments to ensure that their essential functions are performed in the event of an emergency or disaster.

Coordination—The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment. (Criminal Intelligence Glossary, November 2004)

Crime-Pattern Analysis—A process that looks for links between crimes and other incidents to reveal similarities and differences that can be used to help predict and prevent future criminal activity. (Law Enforcement Analyst Standards, November 2004) An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables. (Criminal Intelligence Glossary, November 2004)

Criminal Investigative Analysis—The use of components of a crime and/or the physical and psychological attributes of a criminal to ascertain the identity of the criminal. (Peterson, 1994, p. 42)

An analytic process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s). (Criminal Intelligence Glossary, November 2004)

Database Integrity—It may be advisable, depending on the sensitivity of the data, to utilize multilevel, secure database products to ensure the safety of data. Additionally, limiting data access via database engine passwords or digital certificates separate from the operating system password adds another layer of security. (Criminal Intelligence Glossary, November 2004)

Deconfliction—The process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime and which provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation. (Criminal Intelligence Glossary, November 2004)

Dissemination (of Intelligence)—The release of information, usually under certain protocols. (Peterson, 1994, p. 271) The process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals. (Criminal Intelligence Glossary, November 2004)

Encryption—Many security practitioners believe that encryption technologies, such as those provided by public key infrastructures (PKI), are an essential component in comprehensive privacy and security solutions. The system operator should choose an encryption solution commensurate with the level of (1) risk of possible interception or disclosure, (2) sensitivity of the data transmitted, and (3) access necessary for authorized users. (Criminal Intelligence Glossary, November 2004)

Evaluation (of Information)—An assessment of the reliability of the source and accuracy of the raw data. (Morris and Frost, 1983, p. 4) All information collected for the intelligence cycle is reviewed for its quality with an assessment of the validity and reliability of the information. (Criminal Intelligence Glossary, November 2004)

Event Flow Analysis—Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event, intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events. (Criminal Intelligence Glossary, November 2004) The compilation and analysis of data relating to events as they have occurred over time allow the analyst to draw conclusions and recommendations based on the analysis. (Peterson, 1994)

Financial Analysis—A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and applications of funds, financial statement analysis, and/or Bank Secrecy Act record analysis. It can also show destinations of proceeds of crime and support prosecutions. (Law Enforcement Analytic Standards, November 2004)

Flow Analysis—The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. It can include timelines, event flow analysis, commodity flow analysis, and

activity flow analysis; it may show missing actions or events that need further investigation. (Law Enforcement Analytic Standards, November 2004)

Freedom of Information Act (FOIA)—The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions. (Criminal Intelligence Glossary, November 2004)

Fusion Center—A collaborative effort of two or more agencies who provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism activity. (Recommended Fusion Center Law Enforcement Intelligence Standards, March 2005)

Inference Development—Drawing conclusions based on facts. (Peterson, 1994, p. 48) The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based upon the use of inductive or deductive logic in the analysis of raw information related to the target. (Criminal Intelligence Glossary, November 2004)

Intelligence (Criminal)—The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature. Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (NCISP, October 2003) The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity. (Criminal Intelligence Glossary, November 2004)

Intelligence Assessment—A comprehensive report on an intelligence issue related to criminal or national security threats available to local, state, tribal, and federal law enforcement agencies. (Criminal Intelligence Glossary, November 2004)

Intelligence Bulletins—A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically SBU and available for distribution to local, state, tribal, and federal law enforcement.

Intelligence Information Reports (IIR)—Raw, unevaluated intelligence concerning "perishable" or time-limited information concerning criminal or national security issues. While the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to sensitive but unclassified information in the report under the tear line. (Criminal Intelligence Glossary, November 2004)

Intelligence-Led Policing—The collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels. (NCISP, October 2003) The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses. (Criminal Intelligence Glossary, November 2004)

Intelligence Process (Cycle)—Planning and direction, collection, processing and collating, analysis and productions, dissemination. (Morehouse, 2001, p. 8) An organized process by which information is gathered, assessed, and distributed in order to fulfill the goals of the intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form. (Criminal Intelligence Glossary, November 2004)

Intelligence Products—Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution. (Criminal Intelligence Glossary, November 2004)

***National Criminal Intelligence Sharing Plan* (NCISP)**—A formal intelligence sharing initiative, supported by the U.S. Department of Justice that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence. The Plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives. (Criminal Intelligence Glossary, November 2004)

Need-to-Know—As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation. (Criminal Intelligence Glossary, November 2004)

Operational Analysis—Identifying the salient features, such as groups of or individual criminals relevant premises, contact points, and methods of communication. (Europol, 200, Insert 3) An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist. (Criminal Intelligence Glossary, November 2004)

Perimeter Security—Routers, firewalls, and intrusion detection systems should be implemented to tightly control access to networks from outside sources. Routers and firewalls filter and restrict traffic based upon very specific access control decisions made by the network operators, thereby limiting the types of unauthorized activities on a network. (Criminal Intelligence Glossary, November 2004)

Physical Security—System and network administrators should tightly control physical access to computer and network hardware. Only authorized members of the technical staff should be allowed access to systems. (Criminal Intelligence Glossary, November 2004)

Planning—The preparation for future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations. (Criminal Intelligence Glossary, November 2004)

Privacy (of Information)—The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal

justice agencies, with use of such information to be strictly limited to circumstances where legal process permits use of the personally identifiable information. (Criminal Intelligence Glossary, November 2004)

Privacy (Personal)—The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual, including his/her communications, associations, and transactions, will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances where legal process authorizes surveillance and investigation. (Criminal Intelligence Glossary, November 2004)

Profile/Criminal Profile—An investigative technique by which to identify and define the major personality and behavioral characteristics of the criminal offender based upon an analysis of the crime(s) he or she has committed. (Criminal Intelligence Glossary, November 2004)

Reliability—Asks the question, "Is the source of the information consistent and dependable?" (Criminal Intelligence Glossary, November 2004)

Requirement—A validated intelligence information need (IIN) submitted to address an intelligence gap. Requirements can be "standing" (normally valid for months or years) or "ad-hoc" (processed as they are identified, normally outside of planned, periodic requirements development and prioritization cycles). (FBI Intelligence Requirements and Collection Management Process, August 2003, p. 9)

Right to Know—Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports. (Criminal Intelligence Glossary, November 2004)

SCI (Sensitive Compartmented Information)—Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency. (Criminal Intelligence Glossary, November 2004) (Referenced on page 54)

SCIF (Sensitive Compartmented Information Facility)—An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed. (Criminal Intelligence Glossary, November 2004)

Sensitive But Unclassified (SBU) Information—Information that has not been classified by a federal law enforcement agency which pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria to only those persons necessary to further the investigation or to prevent a crime or terrorist act. (Criminal Intelligence Glossary, November 2004)

Spatial Analysis—The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity. (Criminal Intelligence Glossary, November 2004)

Strategic Intelligence—Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, criminal trend projections, or projective planning. (Law Enforcement Analytic Standards, November 2004) An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems. (Criminal Intelligence Glossary, November 2004)

Tactical Intelligence—Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. (Law Enforcement Analytic Standards, November 2004) Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case. (Criminal Intelligence Glossary, November 2004)

Terrorism—Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience. (Title 22 of the United States Code, Section 2656f(d))

Terrorism Information—All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other United States government activities, relating to 1) the existence, organization, capabilities, plans, intentions, vulnerability, 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; 2) threats posed by such groups or individuals to the United States, U.S. citizens, or U.S. interests, or to those of other nations; 3) communications of or by such groups or individuals; or 4) information relating to groups or individuals reasonably believed to be assisting or associated with such groups or individuals (Executive Order 13356).

Threat Assessment—A strategic document which looks at a group's propensity for violence or criminality or the possible occurrence of a criminal activity in a certain time or place. (Peterson, 1994, pp. 56-57) An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat. (Criminal Intelligence Glossary, November 2004)

Validity—Asks the question, "Does the information actually represent what we believe it represents?" (Criminal Intelligence Glossary, November 2004)

Vulnerability Assessment—A strategic document which views the weaknesses in a system that might be exploited by a criminal endeavor. (NCISP, October 2003) An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack. (Criminal Intelligence Glossary, November 2004)

This Page Is Left Blank Intentionally

Appendix E
Acronyms

This Page Is Left Blank Intentionally

Acronyms

ACTIC	Arizona Counter Terrorism Information Center
ATIX	Automated Trusted Information Exchange
CAP	Common Alerting Protocol
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CITCS	Criminal Intelligence Training Coordination Strategy
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CTTWG	Counter-Terrorism Training Coordination Working Group
DHS	U.S. Department of Homeland Security
DISA	Defense Information Systems Agency
DOJ	U.S. Department of Justice
EPIC	El Paso Intelligence Center
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FinCEN	Financial Crimes Enforcement Network
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GISAC	Georgia Information Sharing and Analysis Center
GISWG	Global Justice Information Sharing Initiative Infrastructure/Standards Working Group
GIWG	Global Justice Information Sharing Initiative Intelligence Working Group
Global	Global Justice Information Sharing Initiative
Global JXDM	Global Justice Extensible Markup Language Data Model
GTRI	Georgia Tech Research Institute
GXSTF	Global XML Structure Task Force
HIDTA	High Intensity Drug Trafficking Areas
HIFCA	High Intensity Financial Crime Areas
HSAC	Homeland Security Advisory Council

HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directives
IACA	International Association of Crime Analysts
IACP	International Association of Chiefs of Police
IADLEST	International Association of Directors of Law Enforcement Standards and Training
IAIP	Information Analysis and Infrastructure Protection
IALEIA	International Association of Law Enforcement Intelligence Analysts
ICSIS	Integrated Convergence Support Information System
IJIS	Integrated Justice Information System
INTERPOL	International Criminal Police Organization
JICC	Justice Intelligence Coordinating Council
LEIN	Law Enforcement Intelligence Network
LEIU	Law Enforcement Intelligence Unit
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive
MOU	Memorandum of Understanding
NCISP	*National Criminal Intelligence Sharing Plan*
NCJA	National Criminal Justice Association
NDIC	National Drug Information Center
NIST	National Institute of Standards and Technology
NLETS	The International Justice and Public Safety Information Sharing Network
NW3C	National White Collar Crime Center
OASIS	Organization for the Advancement of Structured Information Standards
OEP	Occupant Emergency Plan
OJP	Office of Justice Programs
RCIC	Rockland County Intelligence Center
RISS	Regional Information Sharing Systems®
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SOA	Service-Oriented Architecture

STTAC	State Terrorism Threat Assessment Center (California)
STIC	Statewide Terrorism Intelligence Center (Illinois)
TRS	Terrorism Research Specialists
UNYRIC	Upstate New York Regional Intelligence Center
VICAP	Violent Criminal Apprehension Program
XML	Extensible Markup Language

Fusion Center Guidelines

Developing and Sharing Information and Intelligence in a New World

Law Enforcement Intelligence Component

www.it.ojp.gov

For more information, call (850) 385-0600

July 2005

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.