Fusion Center Guidelines

Developing and Sharing Information and Intelligence in a New Era

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

Law Enforcement Intelligence, Public Safety, and the Private Sector

Executive Summary

United States
Department of Justice

Fusion Center Guidelines

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

Through the support, expertise, and knowledge of leaders from all entities involved, 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 requires not only 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 various elements of an ideal information and intelligence sharing project: fusion centers (or "center"). This initiative offers guidelines and tools to assist in the establishment and operation of 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 partners 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.

The development of guidelines for fusion centers was separated into three phases—law enforcement intelligence, public safety, and the private sector. These guidelines may be used for homeland security efforts, as well as all crimes.

What Is the Fusion Center Guidelines Initiative?

In 2004 and 2005, many states began creating fusion centers with various local, state, and federal funds. At the time, no standards or guidelines were in existence to assist with interoperability and communication issues with other centers at the state, regional, and federal levels. As a result, centers designed to share information were actually silos of information, incapable of information exchange. In response, the U.S. Department of Justice (DOJ), at the request of its Global Justice Information Sharing Initiative's (Global) Criminal Intelligence Coordinating Council (CICC), formed the Law Enforcement Intelligence Fusion Center Focus Group (FCFG).[1]

Concurrently, the U.S. Department of Homeland Security's (DHS) Homeland Security Advisory Council (HSAC or Council) Intelligence and Information Sharing Working Group was focusing 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 (i.e., the fusion process). The recommendations resulting from DOJ's initiative and HSAC's efforts laid the foundation for the expansion of the *Fusion Center Guidelines* to integrate the public safety and private sector entities.

Subsequent to publishing Version 1 of the *Fusion Center Guidelines* and the HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report, DOJ and HSAC established two additional focus groups—the Public Safety FCFG and the Private Sector FCFG—in an effort to develop a comprehensive set of guidelines for fusion centers. Participants in the three focus groups included experts and practitioners from local, state, and federal law enforcement agencies; public safety agencies; and the private sector as well as representatives from currently

1 Previously named the Fusion Center Intelligence Standards Focus Group.

operating fusion centers.[2] In addition, representatives from national law enforcement, public safety, and private sector organizations participated in the focus groups.

Fusion refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry.

These guidelines should be used to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities. The 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, the guidelines will help administrators develop policies, manage resources, and evaluate services associated with the jurisdiction's fusion center.

The guidelines should be used for homeland security, as well as all crimes and hazards. The full report contains an in-depth explanation of the guidelines and their key elements. Also included in the report are additional resources, model policies, and tools for guideline implementation.

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 all levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation

The fusion process turns information and intelligence into actionable knowledge.

of risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate or emerging threat-related circumstances and events.

2 Information on currently operating fusion and intelligence centers can be accessed via the National Criminal Intelligence Resource Center at www.ncirc.gov.

Data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector—and, with analysis, can result in meaningful and actionable intelligence and information. The fusion process turns this information and intelligence into actionable knowledge. Fusion also allows for relentless reevaluation of existing data in context with new data in order to provide constant updates. The public safety and private sector components are integral in the fusion process because they provide fusion centers with crime-related information, including risk and threat assessments, and subject-matter experts who can aid in threat identification. Because of the privacy concerns that attach to personally identifiable information, it is not the intent of fusion centers to combine federal databases containing personally identifiable information with state, local, and tribal databases into one system or warehouse. Rather, when a threat, criminal predicate, or public safety need is identified, fusion centers will allow information from all sources to be readily gathered, analyzed, and exchanged, based upon the predicate, by providing access to a variety of disparate databases that are maintained and controlled by appropriate local, state, tribal, and federal representatives at the fusion center. The product of this exchange will be stored by the entity taking action in accordance with any applicable fusion center and/or department policy, including state and federal privacy laws and requirements.

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 analyzing data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (hereafter, NCISP or Plan).[3] The NCISP is 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. It embraces intelligence-led policing, community policing, and collaboration and serves as the foundation for the *Fusion Center Guidelines*.

A *fusion center* is defined as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." Among the primary focuses of fusion centers are the intelligence and fusion processes, through which information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional

3 The *National Criminal Intelligence Sharing Plan* is available at www.it.ojp.gov.

collectors of intelligence, such as public safety entities and private sector organizations, possess important information (e.g., risk assessments and suspicious activity reports) that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity. It is recommended that the fusion of public safety and private sector information with law enforcement data be virtual through networking and utilizing a search function. Examples of the types of information incorporated into these processes are threat assessments and information related to public safety, law enforcement, public health, social services, and public works. Federal data that contains personally identifiable information should not be combined with this data until a threat, criminal predicate, or public safety need has been identified. These processes support efforts to anticipate, identify, prevent, monitor, and respond to criminal activity. Federal law enforcement agencies that are participating in fusion centers should ensure that they comply with all applicable privacy laws when contemplating the wholesale sharing of information with nontraditional law enforcement entities.

In their January 2006 survey, the National Governors Association Center for Best Practices revealed that states ranked the development of state intelligence fusion centers as one of their highest priorities.

Ideally, the fusion center involves every level and 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. The fusion process should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law enforcement intelligence component, center leadership should evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in the fusion center. To aid in this assessment, functional categories have been developed, in which similar entities are grouped. These categories are not comprehensive but represent a starting point for fusion center leadership to begin assessing what agencies and organizations should be involved in the center's operations.

The functional categories include:

- Agriculture, Food, Water, and the Environment
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Criminal Justice
- Education
- Emergency Services (non-law enforcement)
- Energy
- Government
- Health and Public Health Services
- Hospitality and Lodging
- Information and Telecommunications
- Military Facilities and Defense Industrial Base
- Postal and Shipping
- Private Security
- Public Works
- Real Estate
- Retail
- Social Services
- Transportation

The *Fusion Center Guidelines* report contains an appendix describing the functional categories and provides examples of the types of information that the entities can provide to fusion centers.

Why Should Fusion Centers Be Established?

The ultimate goal is to provide a mechanism through which government, 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. It is 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, in order to enhance information and intelligence sharing.

Summary of Guidelines and Key Elements[4]

1. Adhere to the tenets contained in the *National Criminal Intelligence Sharing Plan* (NCISP) and other sector-specific information sharing plans, and perform all steps of the intelligence and fusion processes.

- Consult the tenets of the NCISP, and use model standards and policies as a blueprint for establishing or enhancing the intelligence function within the center.
- Consult the Homeland Security Advisory Council's (HSAC) *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report when incorporating the fusion process in 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 that includes law enforcement, public safety, and the private sector.

- 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, public safety agencies, and the private sector.

- Maintain a diverse membership to include representatives from local, state, tribal, and federal law enforcement, public safety, and the private sector.
- Conduct regular meetings with center personnel, and participate in networking groups and organizations.
- Educate and liase with elected officials and community leadership to promote awareness of center operations.

5. Utilize Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.

- Educate and consult legal advisors early in the fusion center development process.
- Utilize an NDA for fusion center personnel and participants to aid in the security of proprietary information.
- Ensure awareness of local, state, and federal public records laws as they relate to NDAs, including the Freedom of Information Act (FOIA).
- Use an MOU as 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, systems, and networks 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

4 Electronic versions of the documents, products, and reports referenced in the following guidelines can be found at www.it.ojp.gov.

Summary of Guidelines and Key Elements

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's (FBI) Law Enforcement Online (LEO) system, the U.S. Department of Homeland Security's (DHS) 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 U.S. Department of Justice's (DOJ) Global Justice Extensible Markup Language (XML) Data Model and the National Information Exchange Model (NIEM) standards for future database and network development, and consider utilizing the Justice Information Exchange Model (JIEM) for enterprise 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.
- 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.
- Develop rules on the use of privately held data systems information.
- Adhere to applicable state and federal constitutional and statutory privacy and civil liberties provisions.
- Specify that public safety and private sector databases should not be combined with any federal databases that contain personally identifiable information.
- Fusion center participants should comply with all local, state, tribal, and federal privacy laws, when applicable.

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 to Justice Information Sharing* document and resource materials when developing a security plan.
- Consult the Homeland Security Information Act of 2002: Critical Infrastructure Information Act when collecting and storing critical infrastructure-related information.
- Consult private industry security personnel when obtaining and storing industry-specific information (e.g., building security plans).
- Ensure state laws allow for the security and confidentiality of public and private sector data.

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.
- Identify subject-matter experts from the private sector for utilization when industry-specific threats or crimes are identified (e.g., cyber threats).
- 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.
- Include cross-educational training regarding the fusion centers and the applicable functional categories, including the types of information that entities can provide to the fusion center and what the center does with the information, once received.

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, including policymakers, agency heads, and private sector executives.
- 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.
- Ensure that feedback from participating agencies and organizations occurs when products are created and distributed.

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 that 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, tribal, federal, and nongovernmental sources.
- Establish an operational budget and adhere to reporting requirements.

18. Develop and implement a communications plan among fusion center personnel; all law enforcement, public safety, and private sector agencies and entities involved; and the general public.

- Determine primary and secondary modes of communication between the fusion center and participating entities.
- Incorporate regular testing of the plan to ensure its functionality.
- Include a mechanism to alert fusion center participants of new information and intelligence.

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

A companion CD has been developed in conjunction with the *Fusion Center Guidelines* report. This CD contains sample policies, checklists, resource documents, and links to Web sites that are referenced throughout the report. For copies of the resource CD, contact DOJ's Global at (850) 385-0600.

The fusion center resources are also available at DOJ's Global Web site, www.it.ojp.gov/fusioncenter, DHS's Web site, and the Homeland Security Information Network (HSIN).

For more information about the *Fusion Center Guidelines*, contact DOJ's Global at (850) 385-0600.

For more information about DOJ's initiatives, go to

www.it.ojp.gov.

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 and the U.S. Department of Homeland Security. 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 or the U.S. Department of Homeland Security.

Issued
August 2006