DHS/DOJ Fusion Process Technical Assistance Program and Services

Considerations for Fusion Center and Emergency Operations Center Coordination

Comprehensive Preparedness Guide (CPG) 502

May 2010

FEMA

Global Justice Information Sharing Initiative

United States Department of Justice

Preface

Fusion centers and emergency operations centers (EOCs) should become familiar with each others' roles and capabilities to facilitate successful interfacing and cooperation between them. In addition, it is imperative that the two develop a solid relationship in order to effectively work together to achieve their respective objectives. The relationships forged between these two entities will allow them to have continuous, meaningful contacts, which will enhance their ability to share information and intelligence regardless of the activation status of the EOC. Mutual trust and respect must guide interagency collaboration policies and protocols, allowing for effective and consistent collaboration during the steady state or during an emergency.

In addition to addressing the relationship in a concept of operations (CONOPS) and standard operating procedures (SOPs), memorandums of understanding (MOUs) should be created, reviewed and updated to define roles during both periods of activation and non-activation. SOPs and MOUs also define how information will be shared between the two entities. *Comprehensive Planning Guide (CPG) 502* focuses on this critical partnership and the exchange of information between these entities.

Partnerships

Effective prevention, protection, response and recovery efforts depend on the ability of all levels and sectors of government, as well as the private sector, to collect, analyze, disseminate and use homeland security- and crime-related information and intelligence. In support of this, the *National Strategy for Information Sharing* calls for a national information sharing capability through the establishment of a national integrated network of fusion centers. To facilitate the development of a national fusion center capability, the U.S. Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA) National Preparedness Directorate (NPD) and the U.S. Department of Justice's (DOJ) Bureau of Justice Assistance (BJA) have partnered to develop the Fusion Process Technical Assistance Program. This program has been developed in support of the DHS Office of Intelligence and Analysis (I&A) and in coordination with the Office of the Director of National Intelligence (ODNI); the Office of the Program Manager, Information Sharing Environment (PM-ISE); the Federal Bureau of Investigation (FBI) and experts from the State and local community, including the Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC) and the Global Intelligence Working Group (GIWG). The Fusion Process Technical Assistance Program has also been developed to directly support the implementation of the *Fusion Center Guidelines* and the *Baseline Capabilities for State and Major Urban Area Fusion Centers*.

In constructing the *Fusion Center Guidelines*, Global engaged diverse representation from the public and private sectors, melding emergency management and law enforcement expertise. Executive branch partners, such as the ODNI and the PM-ISE, have clarified policies and procedures that guide information sharing.

The process of creating guidance for the operation of fusion centers has evolved through the development of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*. This document identifies the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities. The sustained Federal partnership with State and major urban area fusion centers is critical to the safety of the nation. The baseline capabilities recommend developing processes that govern official outreach with leaders and policymakers, the public sector, the media and citizens. These capabilities also recommend development of a plan to promote awareness of the fusion center's purpose, mission and

functions (which, in turn, enhances partnership with the EOC), as well as ensure a common understanding of roles and responsibilities.

Acknowledgements

A working group of emergency managers, law enforcement agency representatives, fusion center representatives and emergency management and intelligence researchers developed CPG 502 in conjunction with DHS/FEMA and the joint DHS/DOJ Fusion Process Technical Assistance Program. The group and subsequent review sessions included representatives from:

National and Federal Entities

- CPG Working Group
- DHS Office of Intelligence and Analysis
- DHS FEMA National Preparedness Directorate
- Fusion Center Management Group
- Criminal Intelligence Coordinating Council
- National Fusion Center Association

Industry, Research Organizations and Universities

- Argonne National Laboratory: Center for Integrated Emergency Preparedness
- Booz Allen Hamilton
- Community Research Associates, Inc.
- IEM, Inc.
- Lafayette Group

Contents

Introduction and Overview

The fusion process is a cornerstone for the effective prevention of threats, including terrorism and other crimes, by State, local, tribal, and territorial governments. The term "fusion" refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and the private sector. It goes beyond establishing an information/intelligence center or creating a computer network. Many fusion centers have undertaken an all-crimes and/or all-hazards approach, as well as the inclusion of multi-disciplinary and non-law enforcement partners in their processes. Ultimately, the fusion process supports the implementation of risk-based, information-driven prevention, protection, response and recovery programs. At the same time, it supports efforts to address immediate or emerging threat-related circumstances and events.

Multiagency Coordination (MAC)/EOC Management: The capability to activate and sustain EOC/MAC operations, coordinate with other agencies and stakeholders, develop priorities and strategies to support incident management and continuity operations, manage resources and liaison with other entities to coordinates resources, and support executive decision making and coordination of information.

The overall goal of the fusion process is to convert raw information and intelligence into actionable knowledge. Fusion centers are effective mechanisms for guiding this process. Additionally, a national network of fusion centers is working with Federal agencies and the intelligence community to accomplish the National Priorities of *Expanded Regional Collaboration* and *Information Sharing and Collaboration* as defined by DHS's National Preparedness Guidelines. The National Preparedness Guidelines provide a capabilities-based preparedness process and doctrine with planning applications. The guidelines specifically reference the Target Capabilities List (TCL) as a comprehensive catalog of capabilities to perform homeland security missions, including EOC management and intelligence functions. The TCL helps ensure that operational planners and program managers across the nation can use common tools and processes when making planning, training, equipment, and other investments and can produce measurable results.

Emergency Operations Center: The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire services, law enforcement, medical services), by jurisdiction (e.g., Federal, State, regional, tribal, city, county) or by some combination thereof.

EOCs and watch/warning centers, as well as other public safety and first responder agencies and private-sector entities, are essential providers of raw information, operational emergency management information, all-hazards intelligence and other subject matter expertise. In addition, they are users of operational information and intelligence and, therefore, also "customers" of fusion centers.

Coordination of EOCs and fusion centers is crucial to improving the safety of the public. Fusion centers, EOCs and other homeland security entities need to develop positive relationships and establish policies and protocols to share relevant information and intelligence during daily operations and during incidents. In many instances, past efforts to achieve this level of coordination have been met with a concern about how to share information based on its classification level. Conversely, fusion center staff members are often unaware of the type of information the

EOC staff need on a day-to-day basis or during incidents. Successful implementation of these information requirements necessitates willing partners (who understand each other's needs and concerns as well as legal restrictions that may limit the dissemination of law enforcement, medical or other sensitive information) and the establishment of appropriate communication channels. Ultimately, this improved relationship will serve to support a more coordinated, timely and effective response to emerging incidents or threats, as well as the integration of law enforcement-focused prevention efforts with emergency management-focused efforts.

Purpose

This document provides State and Major Urban Area fusion center and EOC officials with guidance for coordination between fusion centers and EOCs. It outlines the roles of fusion centers and EOCs within the fusion process and provides steps by which these entities can work together to share information and intelligence on an ongoing basis. This guide supports the implementation of the *Baseline Capabilities for State and Major Urban Area Fusion Centers* and, likewise, assists EOCs fill their missions in both steady state and active state emergency operations, as supported by the *CPG 601: Design and Management of Emergency Operations Centers*. This CPG provides guidance on the broad capability requirements of an EOC.

Applicability and Scope

This guide is intended for public safety leaders, including emergency management and fusion center personnel. The guide recognizes that many jurisdictions across the country have already developed working relationships and sharing protocols and therefore does not establish any immediate requirements. Rather, this guide suggests that future coordination efforts take this guidance into account.

Authorities

The following Federal legislation, plans and strategies have been critical to the development of information sharing processes:

- Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007
- National Response Framework (NRF)
- National Incident Management System (NIMS)
- National Criminal Intelligence Sharing Plan
- National Strategy for Information Sharing
- Fusion Center Guidelines
- Baseline Capabilities for State and Major Urban Area Fusion Centers
- Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers
- Information Sharing Environment (ISE) Implementation Plan
- ISE Guideline 2
- National Preparedness Guidelines

- CPG 601: Design and Management of Emergency Operations Centers

Public Law 110-53 (also known as "Implementing Recommendations of the 9/11 Commission Act of 2007"). This act established the Urban Area Security Initiative (UASI) to provide grants to assist high-risk metropolitan areas in preventing, preparing for, protecting against and responding to terrorist acts. This law also established the State Homeland Security Grant Program (HSGP) and called for funding for law enforcement and terrorism prevention activities, including information sharing and analysis, target hardening, threat recognition and terrorist interdiction.

NRF, Emergency Support Function (ESF) 5 (Emergency Management). ESF-5 coordinates emergency management and response efforts. It facilitates information flow in the pre-incident phase and coordinates intergovernmental planning, training and exercising in order to prepare assets for deployment. ESF-5 activities include critical functions that support and facilitate multiagency planning and coordination for operations involving incidents requiring Federal coordination, including functions such as information collection, analysis and management.

NRF, ESF-13 (Public Safety and Security). ESF-13 facilitates coordination of public safety and security among Federal, State, local, tribal, and territorial agencies to ensure that communication and coordination processes are consistent with stated incident management missions and objectives. ESF-13 is generally activated when extensive assistance is required due to inadequate or overwhelmed State, local, tribal, and territorial resources or when protective solutions or capabilities unique to the Federal Government are required, especially in pre- or post-incident situations. When activated, ESF-13 may provide protection and security resources, planning assistance, technology support and other technical assistance to support incident operations.

NIMS. NIMS is a set of principles that provides a systematic, proactive approach for guiding government agencies at all levels, nongovernmental organizations and the private sector to work seamlessly to prevent, protect against, respond to, recover from and mitigate the effects of incidents, regardless of cause, size, location or complexity in order to reduce the loss of life or property and harm to the environment.

National Criminal Intelligence Sharing Plan. The National Criminal Intelligence Sharing Plan was first published in October 2003 and revised in July 2005. The purpose of the plan is to link Federal, State, local, tribal, and territorial law enforcement agencies, allowing them to share intelligence information to prevent terrorism and crime. The plan outlines policies, standards and guidelines for developing a local law enforcement intelligence function and includes recommendations regarding key implementation issues and barriers. It also emphasizes better methods for developing and sharing critical data. The CICC was established to set national-level policies to implement the plan and to monitor its progress on the State and local levels. The CICC works with the Law Enforcement Information Strategy Initiative of DOJ and with the Justice Intelligence Coordinating Council to improve the flow of intelligence and information among all levels of law enforcement agencies.

National Strategy for Information Sharing. This strategy adheres to the National Security Strategy and is closely aligned with the National Strategy for Combating Terrorism, the National Intelligence Strategy and the National Strategy for Homeland Security. The strategy describes the Administration's plan to establish a more integrated information sharing capability, improve interagency information sharing at the Federal level and build information sharing between the Federal Government and non-Federal partners. The strategy is founded on the following guiding principles:

- Effective information sharing comes through strong partnership among Federal, State, local, tribal, and territorial authorities, private-sector organizations and foreign partners and allies.

- A cultural awareness must be fostered to use information and knowledge from all sources to support counterterrorism efforts.
- Information sharing must be integrated into all aspects of counterterrorism activity.
- Information sharing procedures, processes and systems must draw upon and integrate existing technical capabilities and respect established authorities and responsibilities.
- State and major urban area fusion centers need to be incorporated into the national information sharing framework.

Fusion Center Guidelines - DOJ, in collaboration with DHS and the FBI, developed these guidelines for law enforcement, intelligence, public safety and private-sector communities to effectively implement ways to develop and operate fusion centers throughout the country. The guidelines make specific recommendations on law enforcement roles, governance, information technology (IT) needs and information security to better protect our homeland and maximize crime-fighting efforts.

Baseline Capabilities for State and Major Urban Area Fusion Centers. As an addendum to the *Fusion Center Guidelines*, this document identifies baseline capabilities and operational standards necessary for fusion centers to achieve their objectives. Baseline capabilities are labeled under *Fusion Process Capabilities* and *Management and Administrative Capabilities*.

CIKR Protection Capabilities for Fusion Centers. As an appendix to Global's *Baseline Capabilities for State and Major Urban Area Fusion Centers*, this document identifies the capabilities necessary for State and major urban area fusion centers to establish a CIKR protection analytic capability that supports infrastructure security activities at the State and local levels.

ISE Implementation Plan. Authorized under the Intelligence Reform and Terrorism Prevention Act of 2004, the plan identifies and promotes procedures on information sharing to facilitate anti- and counterterrorism efforts amongst the Federal, State, local, tribal, and territorial governments and other ISE partners.

ISE Guideline 2. Authorized under the Intelligence Reform and Terrorism Prevention Act of 2004, the guideline develops a common framework for information sharing between and among Federal departments and agencies, as well as State, local, tribal, and territorial governments, law enforcement agencies and the private sector. It requires the development and implementation of this framework for "homeland security information," "terrorism information," and "law enforcement information."

National Preparedness Guidelines. Implemented under the authorization of Homeland Security Presidential Directive (HSPD) 8, these guidelines supersede the National Preparedness Goal and define how to prepare for all hazards. It organizes and synchronizes efforts across the country to strengthen the nation's preparedness by reinforcing the concept that preparedness is a shared responsibility.

CPG 601: Design and Management of Emergency Operations Centers (*release date TBD*). CPG 601 is a new Federal guidance document designed to address the broad capability requirements of an EOC. It supersedes *Civil Preparedness Guide 1-20, Emergency Operations Center Handbook*, which was written in 1984 and revised in 1989. *Civil Preparedness Guide 1-20* is rescinded.

How to Use This Guide

This document is part of the joint DHS/DOJ Fusion Process Technical Assistance Program and the broader FEMA CPG effort and is designed to help both novice and experienced planners navigate the planning process. The first section addresses the applicability, authority, purpose and scope of this CPG. The next section outlines the roles and initiatives of Federal departments. The third and fourth sections detail how fusion centers and EOCs function, within the broader context of the information sharing environment. The fifth section describes how fusion centers and EOCs may consider coordinating with each other for intelligence and information sharing, and the last section provides case studies about this coordination. The appendices to this guide are as follows:

- Appendix A: Glossary and Acronyms
- Appendix B: Draft Memorandum of Understanding
- Appendix C: Fusion Center and EOC Interface: Analysis of Coordination and Integration Best Practices
- Appendix D: Developing Processes to Acquire and Use Geospatial Information to Support All-Hazards Planning and Response
- Appendix E: Public-Private Partnerships: Safeguard Iowa Partnership's Code of Conduct Manual for Liaisons Serving at Emergency Operations Centers

NIMS Compliance and Integration

NIMS provides guidance on utilizing and integrating the Intelligence/Investigations function. The Intelligence/ Investigations function within the Incident Command System (ICS) provides a flexible and scalable framework that will allow for the integration of intelligence and investigations activities and information. Figure 1 delineates the places in which the information and intelligence function may be found within an incident command structure and allows for the Operations section to be supported by fusion center personnel.

Based on the incident needs, the information and intelligence function may be activated as a fifth section, as an element within the Operations or Planning Sections or as part of the Command Staff.

See NIMS for additional information.

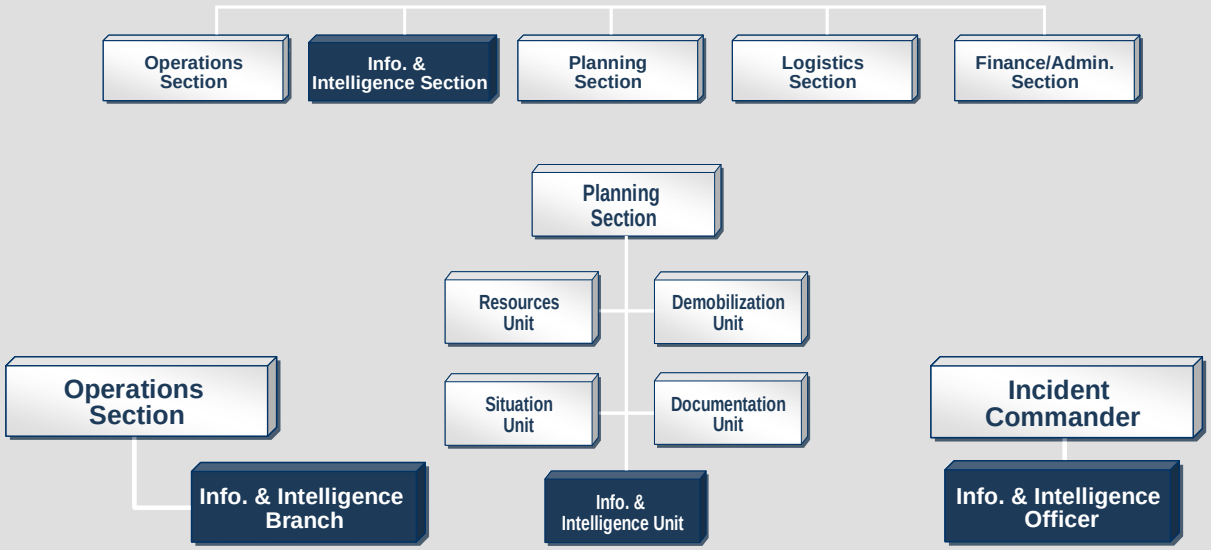


Figure 1: Possible Placement of the Information and Intelligence Unit within a Command Structure

Although the emergency management system and fusion center network may use different methods and tools, both share a public safety mission. Integrating the concepts of NIMS and the ISE can contribute toward effective collaboration in the joint mission space.

Recommended Training

See EOC and Fusion Center Coordination: Step Four: Training, Workshops and Exercises.

Revision Process

DHS will revise this CPG as needed and issue changed pages through the publication and distribution system and online through a variety of sources (e.g., Disaster Assistance [http://www.disasterassistance.gov] and DHS Lessons Learned Information Sharing (LLIS) [http://www.llis.dhs.gov]).

DHS welcomes recommendations on how to improve this CPG so it better serves the needs of the homeland security, law enforcement, and emergency management communities. Recommendations for improving this guide can be sent to NPD-Planning@dhs.gov, ATTN: PAB – CPG Initiative – 502.

Federal Departments Initiatives, Roles and Guidelines

Federal Initiatives and Roles

Fusion Center Management Group

The Fusion Center Management Group is co-chaired by DHS Office of Intelligence and Analysis (I&A) and the Office of the Program Manager, Information Sharing Environment (PM-ISE). The mission of this group is to provide leadership, coordination and guidance in the development of—and the Federal government's support to—a national integrated network of fusion centers operating at the defined baseline level of capability. The following are goals of the group:

- Serve as the primary forum for coordinating Federal support in the development, support and sustainment of a national, integrated network of State and major urban area fusion centers operating at a defined baseline level of capability;
- Promote awareness of fusion centers' mission, purpose and value among internal and external stakeholders; and
- Develop a coordinated strategy for the sustainment of fusion centers.

Department of Homeland Security

The Secretary of Homeland Security identified I&A as the executive agent within DHS for coordinating the Department's activities with fusion centers. As a member of both the intelligence community and DHS, I&A provides a vital link between the intelligence community and Federal, State, local, tribal, territorial, and private sector entities. It works closely with the 16 Federal intelligence organizations and agencies, as well as local, tribal, territorial, and private-sector entities to ensure information and intelligence are collected, fused, analyzed and disseminated to all related partners, as necessary and appropriate, to provide a complete assessment of the threats across the country. It works with fusion centers throughout the country against threats and hazards related to a variety of issues and situations, including border security, radicalization and extremism, particular groups entering the United States, protection of CIKR and weapons of mass destruction (WMD). DHS also created a program office within I&A to address the concerns of State and local officials and to manage deployment of personnel and other resources to fusion centers.

FEMA provides support to DHS I&A to assist with the development, implementation and operation of fusion centers through the joint DHS/DOJ Fusion Process Technical Assistance Program. This effort includes coordination of related fusion center efforts with specific DHS offices, including the DHS Office

of Infrastructure Protection (IP), DHS Office of Health Affairs (OHA), the U.S. Fire Administration (USFA) and others. FEMA also supports the development and operation of EOCs to improve emergency management and preparedness capabilities at the Federal, State, local, tribal, territorial, and private-sector level through the provision of support via the EOC Design and Management Technical Assistance service and by supporting NIMS compliance. The NIC provides strategic direction and a national program for NIMS education and awareness throughout the country.

Department of Justice, Bureau of Justice Assistance

BJA is a component of the DOJ Office of Justice Programs and supports law enforcement, corrections, technology and other related prevention initiatives that strengthen the nation's criminal justice system. BJA has three primary components: policy, programs and planning. The Policy Office provides national leadership in criminal justice policy, training and technical assistance to further the administration of justice. It also acts as a liaison to national organizations that partner with BJA to set policy and help disseminate information on best and promising practices. The Programs Office coordinates and administers all State and local grant programs and acts as BJA's direct line of communication to State, local, tribal, and territorial governments by providing assistance and coordinating resources. The Planning Office coordinates the planning, communications and budget formulation and execution; provides overall BJA-wide coordination and supports streamlining efforts. BJA also supports the management of the joint DHS/DOJ Fusion Process Technical Assistance Program, which supports the development, implementation and operation of fusion centers.

Global Justice Information Sharing Initiative and the Criminal Intelligence Coordinating Council

Established in May 2004, Global's CICC is composed of members from law enforcement agencies at all levels of government. Members of the CICC serve as a significant voice and advocates for State, local, tribal, and territorial law enforcement and fusion centers, supporting their efforts to develop and share criminal intelligence. Because of the indispensable part that State, local, tribal, and territorial law enforcement play in homeland security, it is imperative that they have a voice in the development of policies and systems for information and intelligence sharing. The CICC is in the unique position to ensure these voices are heard and advises the U.S. Attorney General on the best use of criminal intelligence to keep the United States safe.

The Role of Fusion Centers

As defined by the *Fusion Center Guidelines*, a fusion center is 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. The primary products of a fusion center are situational awareness and warnings that are supported by law enforcement intelligence, derived from the application of the intelligence process, where requirements for actionable information are generated and information is collected, integrated, evaluated, analyzed and disseminated."

The Intelligence Process

The core function of a fusion center is the intelligence process. Simply stated, the intelligence process (or cycle) is an organized process by which information is gathered, assessed and distributed. Figure 2 depicts the following steps in the process: planning and direction, information gathering, processing and collation, analysis and production, dissemination and reevaluation (feedback). Fusion centers engage in this process, regardless of their mission (all-crimes, terrorism or all-hazards), the disciplines or stakeholders they support (law enforcement, fire services, public health, etc.) or the types of information they receive. This process is the means by which raw information becomes a finished intelligence product for use in decision making and formulating policies/actions.

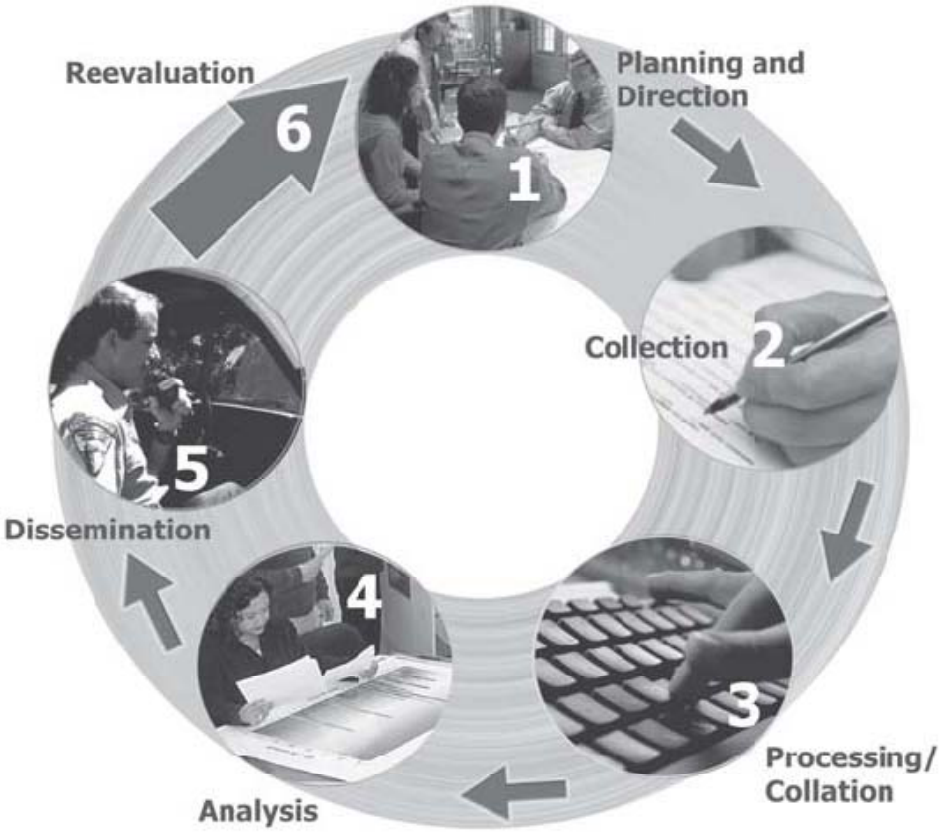


Figure 2: Intelligence Process

The Fusion Process: Turning Information and Intelligence into Actionable Knowledge

The term "fusion" refers to managing the flow of information and intelligence across levels and sectors of government and the private sector. It goes beyond establishing an intelligence center or creating a computer network. Fusion supports the implementation of risk-based, information-driven prevention, response and consequence management programs. At the same time, the fusion process supports efforts to address immediate or emerging threat-related circumstances and events. Data fusion involves the exchange of Federal and non-Federal information from different sources, including law enforcement, public safety and the private sector. When combined with appropriate analyses, data fusion results in meaningful and actionable intelligence and information. Thus, the fusion process turns information and intelligence into knowledge.

Information vs. Intelligence

- **Information:** Pieces of raw, unanalyzed data or reports from various sources about an event, criminal activity or subject of interest.
- **Intelligence:** The product of the collation, evaluation and analysis of raw information with respect to an identifiable person or group of persons in an effort to anticipate, prevent or monitor possible threats (i.e., criminal, terrorist or naturally occurring activity).

"Intelligence is information that has been analyzed to determine its meaning and relevance."

The fusion process also:

- Allows State, local, tribal, and territorial entities to better forecast and identify emerging crime, public safety and public health trends;
- Supports multidisciplinary, proactive, risk-based and community-focused problem solving;
- Provides a continuous flow of intelligence to officials to assist in developing a depiction of evolving threats or hazards; and
- Improves the delivery of emergency and non-emergency services.

Actionable Intelligence

Intelligence should:

- Paint a picture;
- Tell a story;
- Guide the response; and
- Produce knowledge upon which a course of action can be developed/recommended for resolution.

Fusion Center Guidelines

Each fusion center tailors its scope and mission to meet specific jurisdictional needs, but the *Fusion Center Guidelines* emphasize a consistent framework by which all fusion centers should operate. There are 18 guidelines, and each guideline discusses an expectation for fusion center operations. For example, all fusion centers are encouraged to leverage existing systems, databases and networks (such as DOJ's Global Justice Extensible Markup Language Data Model and the National Information Exchange Model (NIEM) standards). Fusion centers are also expected to adhere to the National Criminal Intelligence Sharing Plan, develop a mission statement to identify goals and promote common terminology for all involved stakeholders.

Baseline Capabilities for State and Major Urban Area Fusion Centers

The *Fusion Center Guidelines* contain an addendum called the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, which provides a series of recommended baseline capabilities and standards or tasks to accomplish their mission. Baseline capabilities are categorized into two sections:

1. Fusion Process Capabilities; and
2. Management and Administrative Capabilities.

The Fusion Process Capabilities section focuses on the intelligence process within the fusion center while the Management and Administrative Capabilities section focuses on the proper management and functioning of the fusion center. They also provide general tenets for integrating the information exchange processes of fusion centers and EOCs, which will be discussed in greater detail in the EOC and Fusion Center Coordination section of this guide.

Fusion Process Capabilities

The Fusion Process Capabilities addresses the intelligence process of the fusion center including intelligence collection, analysis and dissemination (see Figure 2). The intelligence process is the foundation of the fusion process and is necessary for fusion centers to operate. The intelligence process is addressed in each of the following areas:

1. Planning and Requirements Development;
2. Information Gathering/Collection and Recognition of Indicators and Warnings;
3. Processing and Collation of Information;
4. Intelligence Analysis and Production;
5. Intelligence/Information Dissemination; and
6. Reevaluation.

Management and Administrative Capabilities

The Management and Administrative Capabilities focus on proper management and functions of fusion centers. These capabilities create the environment in which centers can operate, assign tasks, allocate and manage resources and develop and enforce policy. The Management and Administrative Capabilities typically include the following functions:

1. Management/Governance;
2. Information Privacy Protections;
3. Security;
4. Personnel and Training;
5. IT/Communications Infrastructure, Systems, Equipment, Facility and Physical Infrastructure; and
6. Funding.

Fusion Center Functions

Fusion centers compile, analyze and disseminate criminal, homeland security and terrorist information and intelligence, as well as information regarding public safety, law enforcement, fire, public health, social services, public works, etc. This intelligence and information is both strategic (i.e., designed to provide guidance on general trends) as well as tactical (i.e., intended for a specific event) and is collected on an ongoing basis. The *National Strategy for Information Sharing* recognizes the sovereignty of the entities that own and/or are considering operating a fusion center. The missions of fusion centers vary based on the environment in which the center operates—some have adopted the all-crimes approach, whereas others have also included an all-hazards approach. The strategy supports and encourages these approaches, while respecting the principle that a fusion center's mission should be defined based on jurisdictional needs.

State, local, tribal, and territorial governments, as well as private-sector entities, are encouraged to work with both State and UASI regions to participate in fusion efforts. The public should also be engaged through public education programs that describe warning signs and actions that should be taken if suspicious activity is observed.

It is critical to the successful coordination between EOCs and fusion centers that the fusion focus is expanded beyond law enforcement. In many States, fusion centers include emergency managers, fire, hazardous materials, public health and other disciplines in their operations or within their liaison or outreach efforts. Generally, these efforts to incorporate other agencies' needs and personnel have been extremely successful and have enhanced the integration of the fusion centers into the entire prevention, protection, response and recovery mission areas. This integration also helps cement the long-term value and viability of the fusion centers in support of emergency management and response.

Fusion Center Baseline Capability: All-Hazards Approach

An all-hazards approach refers to preparedness for terrorist attacks, major disasters and other emergencies within the United States. Within the context of the fusion process, some fusion centers have defined their mission to include an all-hazards approach. While the application of the all-hazards approach varies, it generally means the fusion center has identified and prioritized types of major disasters and emergencies, beyond terrorism and crime that could occur within their jurisdiction. For this approach, fusion centers also gather, analyze and disseminate information that would assist the relevant responsible agencies (e.g., law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response or recovery efforts of those incidents. A fusion center can use an all-hazards approach but not address every possible hazard in its operations. Part of the annual risk assessment a fusion center develops (or supports development of) should identify which hazards a State, Territory, Tribe or region should prioritize within its homeland security planning process. The risk assessment can be used by the fusion centers to formulate their Standing Information Needs (SINs). The SINs, in turn, are used to guide the participants in the fusion process and their information collection efforts.

This page intentionally left blank.

The Role of the Emergency Operations Center

EOCs are the physical location where multi-agency response coordination occurs. Most States maintain a State-level EOC configured to expand, as necessary, to manage events requiring State-level assistance. EOCs help form a common operating picture of the incident, relieve on-scene command of the burden of external coordination and secure additional resources. The core functions of an EOC include coordination, communication, resource allocation and tracking and information collection, analysis and dissemination.

Common Operating Picture: An overview of an incident by all relevant parties that provides incident information enabling the Incident Commander/Unified Command and any supporting agencies and organizations to make effective, consistent, and timely decisions.

EOC Organization and Structure

Civil Preparedness Guide 1-20 was the last Federal guidance written in 1984 to address the broad capability requirements of an EOC. Even though it was revised in 1989, the field of emergency management has changed significantly since then. *Civil Preparedness Guide 1-20* is rescinded and is superseded by *CPG 601: Design and Management of Emergency Operations Centers*. This new Federal planning guide provides information for developing a new EOC or retrofitting an existing one through assessment and needs analysis.

EOCs may be permanent organizations and facilities that are staffed full time, or they may be established to meet short-term needs. Standing EOCs (or those activated to support larger, more complex incidents) are typically established in a central or permanently established facility. Such permanent facilities in a State or larger community are typically directed by a full-time emergency manager. EOCs may be organized by major discipline (fire, law enforcement, medical services, etc.), by jurisdiction (city, county, region, etc.), by ESF (communications, public works, engineering, transportation, resource support, etc.) or, more likely, by some combination thereof.

EOCs may also be staffed by personnel—with varying levels of training and sometimes a collateral duty—representing multiple jurisdictions and functional disciplines and a wide variety of resources. For example, an EOC established in response to a bioterrorism incident would likely include a mix of law enforcement, emergency management, public health and medical personnel (e.g., local, State, or Federal public health officials and possibly representatives of health care facilities, emergency medical services, etc.).

The physical size, staffing and equipping of an EOC will depend on the size of the jurisdiction, resources available and anticipated incident management workload. EOCs may be organized and staffed in a variety of ways. Regardless of its specific organizational structure, an EOC should include the following core functions: coordination; communications; resource allocation and tracking and information collection, analysis and dissemination.

EOC Function

While the local incident command structure directs on-scene incident management activities and maintains command and control of on-scene incident operations, EOCs are activated as necessary to support these local efforts. Therefore, the EOC is the central location from which off-scene activities are coordinated. Additionally, some States may implement and leverage regional operations centers between the local incident command and a State-level EOC. Chief elected and appointed officials, as well as personnel supporting core functions, may be located at the EOC depending upon the responsibilities of their positions. These officials are often members of the policy group and may have primary responsibility for policy decisions. The key function of EOC personnel is to ensure that responders who are located at the scene have the resources (e.g., personnel, information, tools and equipment) they need for the response and to manage public information. Additionally, governmental departments (or agencies, bureaus, etc.) or private organizations may also have department operations centers (DOCs) that serve as the interface between the ongoing operations of that organization and the emergency operations it is supporting. The DOC may directly support the incident and receive information relative to its operations. In most cases, DOCs are physically represented in a combined agency EOC by authorized agents for the department or agency.

Upon activation of an EOC, communication and coordination should be established between Incident Command and the EOC. Additionally, EOCs at all levels of government and across functional agencies should be capable of communicating appropriately with other EOCs, including those maintained by private organizations. Communications systems between EOCs must be reliable and contain built-in redundancies. The efficient functioning of EOCs often relies on the existence of mutual aid agreements and joint communications protocols among participating agencies.

An EOC is activated to support on-scene response during an escalating incident. Activating the EOC relieves the on-scene Incident Commander of the burden of external coordination and securing additional resources.

- An EOC is:
  - A physical location;
  - Staffed with personnel trained for and authorized to represent an agency/discipline;
  - Equipped with mechanisms for communicating with the incident site and obtaining resources;
  - Managed through protocols; and
  - Used by all levels of government.
- An EOC consists of personnel and equipment appropriate to the level of incident.
- An EOC is used:
  - In varying ways within all levels of government and the private sector; and
  - To provide coordination, direction and support during emergencies.
- An EOC may:
  - Facilitate Multiagency Coordination System (MACS) functions and may be needed to support Area Command, Incident Command or Unified Command when resource needs exceed local capabilities;
  - Provide for the transition into recovery; and
  - Be activated in anticipation of an event.
- An EOC does not command the on-scene tactical level of the incident.

EOCs should be both flexible and scalable. They will generally perform common functions during an incident; however, not all of the system's functions will be performed during every incident, and functions may not occur in any particular order. Primary functions may include the following:

- Situation assessment;
- Incident priority determination;
- Critical resource acquisition and allocation;
- Policy direction for relevant incident management and interagency activities;
- Coordination with FEMA Regional Response Coordination Centers (RRCCs);
- Coordination with other MACS elements;
- Coordination with elected and appointed officials;
- Coordination of summary information; and
- Public information.

Multiagency Coordination System: The primary function of the MACS is to coordinate activities above the field level and to prioritize the incident demands for critical or competing resources, thereby, assisting the coordination of the operations in the field. The MACS consists of a combination of elements, such as personnel, procedures, protocols, business practices and communications integrated into a common system.

Operational Exchange of Information

A primary focus of EOCs is on response and recovery efforts associated with natural and man-made incidents. While the purposes of an EOC and a fusion center differ greatly, it is essential for these two entities to work together and to understand each other's goals and priorities, as well as where their missions may be similar or overlap. At a minimum, EOCs should establish close communication with fusion centers for the exchange of actionable information. Fusion center plans and procedures should include information about how the center will support the EOC prior to, during and after an event or incident.

These information exchange processes should begin early in the planning phases (i.e., prior to an incident, by addressing the fusion center's role in the EOP and hazard analysis development phases). During the hazard analysis, the jurisdiction examines hazards that likely to affect the community and risks posed by each hazard are then quantified. When completed, the community's hazard analysis should form the basis for the entire emergency planning process and the development of an EOP. The EOP establishes the overall authority, roles and functions performed during emergencies, is activated to guide emergency response and recovery activities and designates the facility that will serve as the EOC during emergencies.

Depending on jurisdictional responsibilities, fusion centers can play a valuable role in providing information and intelligence to support the completion or update of a hazard analysis and resulting EOP. Additionally, any information about specific incidents or events that may affect the jurisdiction—or would allow the jurisdiction to be better prepared—should be shared with the emergency manager and perhaps with the full EOC staff. EOCs can provide the fusion center with situational awareness of ongoing events and serve as a warning point during activation.

What Is in a Hazard Analysis?

A hazard analysis involves examining the likely hazards that could affect a community and quantifying the risk posed by each hazard. Hazards are conditions or situations that have the potential for causing harm to people, property or the environment. Hazards can be classified into three categories:

- Natural (e.g., tornadoes and earthquakes);
- Intentional (e.g., terrorism or civil disturbance); and
- Technological (e.g., failure of the power grid or hazardous materials spills).

Hazard analysis itself includes three steps:

Step 1: Identifying Hazards. Develop a list of hazards that may occur in a community. This list is usually based on historical data about past events. Sources of information about past events may include newspaper files; weather records; insurance records; accident reports; EOC records; fire department inspections and anecdotal information from long-time residents.

Step 2: Developing Hazard Profiles. Develop a profile of each identified hazard according to the following characteristics:

- Predictability (e.g., frequency and/or likelihood of occurrence, seasonal pattern, etc.);
- Magnitude or severity of impact on the community (e.g., extent of damage expected, the types of damage that can be expected to the infrastructure, etc.);
- Speed of onset (e.g., hurricanes usually provide some amount of preparation time before they strike while earthquakes or explosions could occur without warning); and
- The potential for cascading effects (e.g., flooding following a hurricane or fires following an earthquake because of gas line ruptures).

Step 3: Determining Risk Using a Hazard Analysis. After compiling information for each hazard that a community is vulnerable to, the risks associated with each hazard need to be assessed so that the planning team can predict and prepare for those of highest potential impact on people, services, facilities and structures. When assessing risk, it is important to keep in mind the following hierarchy of response priorities:

1. *Life safety.* Conditions that could affect the health and/or safety of the population;
2. *Essential facilities.* Facilities, such as fire houses, precinct houses or waste water treatment facilities that, if affected by the hazard, would seriously and adversely affect the community's ability to respond; and
3. *CIKR.* Roadways, utilities and other components of the infrastructure that, if damaged, would seriously and adversely affect life safety or response capability.

Because many EOCs have limited staffing resources, intelligence analysts from State or urban area fusion centers may be available to augment the fusion center/EOC interface (physically or virtually) and to serve as liaisons during an incident. The details of the augmentation of EOC staff with fusion center personnel should be included in the MOU between the two centers and should include both the steady state and the active state of EOC operations. In many cases, fusion centers are co-located or located in close proximity with the EOC. EOCs might also consider establishing a task force of personnel assigned to serve as liaisons to the fusion center when the EOC is not activated so that staff can gain familiarly with fusion center activities and operations. In jurisdictions where a fusion liaison program is formalized, a cadre of qualified personnel may already exist.

Steady State: Steady state is the posture for routine, normal, day-to-day watch operations and situational awareness, contrasted by temporary periods of heightened alert or real-time response to threats or incidents.

EOCs should plan to have a capability to access and share information with fusion centers, as well as other entities, and should leverage systems such as the Regional Information Sharing System (RISS), Law Enforcement Online (LEO) and the Homeland Security Information Network (HSIN) to support this. Additionally, EOC's must ensure safeguards are enacted when information from the fusion center is passed. These safeguard measures may include limiting dissemination of information to appropriate personnel assigned to the EOC, signing non-disclosure agreements and ensuring members who have access to this information are vetted for U.S. citizenship and have a need to know.

EOCs also need a host of other information, including weather, geospatial and remote sensing imagery, damage assessments, media reports, financial impact and social effects. They may need assistance in gathering this event- or incident-specific information for planning, response and/or recovery purposes. Fusion center personnel may also be useful in analyzing the information gathered by EOC sources, particularly when the EOC is in the active state and has a greater need for decision-making information.

Information and Intelligence Management: It is important that the incident management organization establishes a process for gathering, sharing and managing incident-related information and intelligence. The following are examples of information and intelligence used to manage an incident:

- Risk assessments;
- Medical intelligence (i.e., surveillance);
- Weather information;
- Geospatial data;
- Structural designs;
- Toxic contaminant levels; and
- Utilities and public works data.

A number of fusion centers are at various stages in developing formalized processes and procedures for requesting, accessing and using geospatial data to support all-hazards planning and response efforts. Useful geospatial data can run the gamut from before/after aerial photography or satellite imagery to point locations of water intakes in a flood plain to the locations of CIKR assets. Fusion centers should engage in thoughtful planning so that they are prepared to request, access and use geospatial resources efficiently.

See Appendix D: Developing Processes to Acquire and Use Geospatial Information to Support All-Hazards Planning and Response for more information.

EOC and Fusion Center Coordination

Coordinating and/or integrating EOC and fusion center operations require careful planning and coordination. The following steps are recommended for this process. Within each step, the associated fusion center baseline capability will be addressed.

Both the fusion center and the EOC bring resources, capabilities, products/reports and concerns to the discussion. Significant planning is required to foster collaborative, long-term working relationships that include training and exercising. Open dialogue from the outset will allow both sides to address concerns and develop a governance mechanism to maintain the process.

Fusion Center Baseline Capabilities:

I. Fusion Process Capabilities:

A. Planning and Requirements Development

8. **Coordination with Response and Recovery Officials.** Fusion centers shall identify and coordinate with emergency managers, appropriate response and recovery personnel and operations centers to develop, implement and maintain a plan and procedures to ensure a common understanding of roles and responsibilities and to ensure that intelligence and analysis capabilities can be leveraged to support emergency management operation activities, as appropriate, when events require such a response.

Step One: Familiarization with Capabilities, Needs and Requirements

Prior to making agreements or developing policy, leaders for the EOC and fusion center should meet to discuss their respective capabilities and needs/requirements.

Each center should prepare for the other a list outlining the capabilities they have, the products, assessments and reports they produce and their informational needs/requirements, standing information needs (SINs) and/or essential elements of information (EEIs). It is especially important that the EOC specify exactly what information or intelligence they need (i.e., their EEIs), why they need it and when they need it. This may vary between normal operating times (steady state) and as an incident builds up, occurs (active state) and eventually returns to steady state. If there are particular timetables established for EOC products, such as briefings or situation reports, the EOC should ensure the fusion center is aware of them. Additionally, the EOC should be able to describe the reports and products they are capable of developing and sharing with the fusion center, especially those relating to all-hazards or naturally occurring incidents.

FEMA National Response Coordination Center (NRCC) Data Elements

FEMA has identified 26 EEIs. Additionally, incident-specific Information Collection Plans (ICPs) have been developed to translate EEIs into specific information requirements.

Essential Elements of Information

- Disaster area boundaries/access points
- Jurisdictional boundaries
- Social/economic/political impacts
- Transportation system status
- Communication system status
- Key Federal/State facility status
- Hazard-specific information
- Significant weather
- Seismic or other geophysical data
- Critical facility status
- Aerial reconnaissance activity status
- Key official status
- ESF activation/deactivation status
- Disaster/emergency declaration status
- ESF major issues/activities
- Resource shortfalls
- Limiting factors
- Response priorities
- Planned or upcoming activities
- Donations

Information Collection Plans

- Earthquake
- Epidemic-Pandemic
- Flood
- Generic
- Hazardous materials
- Hurricane
- Nuclear plant
- Power failure
- Terrorist
- Tornado
- Tsunami
- Volcano
- Winter storm

A candid dialog of each center's needs will provide a greater understanding of the potential constraints that must be overcome to meet those needs. Without this dialog, it would be easy to pass unnecessary or unusable products or information in hopes of sharing enough of the right information. Providing an exchange of timely, accurate and useable information is the key to this successful interaction.

Standard Policies and Procedures

Understanding each other's CONOPS and SOPs will assist the fusion centers and EOCs in formulating a plan to work together. Many fusion centers have created CONOPS and SOPs that incorporate the *Fusion Center Guidelines* and the *Baseline Capabilities*. Those should be shared with the EOC, and new SOPs can be developed to address the working relationships between the two. SOPs are particularly important to new personnel assigned to either entity during a crisis or disaster. During planning sessions, SOPs should be reviewed to ensure they are current. Personnel should be trained on these SOPs, and the SOPs should also be exercised and evaluated to ensure they are accurate and applicable.

Communication Tools

The ability to share information and communicate across a variety of mediums before, during, and after an incident is essential. Therefore, EOCs and fusion centers should review current processes to identify how this communication will occur across all necessary classification levels.

- Which tools are available for EOCs and fusion centers to send, receive and manage information?
  - Are the tools interoperable?
  - Do the tools have limited access rights?
  - Have the tools been exercised?
- What real-time tools are used during an incident?
- Does the fusion center or EOC have the capacity for online information sharing portals? How about email and distribution lists?
  - Can the EOC receive, store and handle classified information?
  - Does the EOC and fusion center have secure communication capabilities?

Fusion Center Baseline Capabilities:

II. Management and Administrative Capabilities:

E. Information Technology / Communications Infrastructure, Systems, Equipment, Facility and Physical Infrastructure

3. Communications Plan—Fusion centers shall have a plan to ensure safe, secure and reliable communications, including policies and audit capabilities. (Guideline 18, Fusion Center Guidelines)

a. Identify how fusion center partners will communicate during an incident or emergency. Ensure that existing communications capabilities are interoperable.

b. Incorporate current communications plans utilized by law enforcement and emergency services.

Databases

What software applications and databases do fusion centers and EOCs use or have access to? Is the software compatible? If so, how will it be linked and for what purposes? If not, should adjustments be made to make it compatible?

- CIKR databases
  - Automated Critical Asset Management System (ACAMS)
- Geographic Information Systems (GIS) Capabilities
- LEO
- RISS
- HSIN

- Homeland Security Data Network (HSDN)
- Virtual EOC or other emergency management software applications
- Public health alert and information sharing systems, such as the Health Alert Network (HAN), the Epidemic Information Exchange (Epi-X), the Public Health Information Network (PHIN) and the National Electronic Disease Surveillance System (NEDSS)
- Situational awareness or watch/warning systems
- Other classified and unclassified IT and intelligence sharing platforms

Staffing

Fusion center staff includes law enforcement officials, as well as intelligence, crime and/or CIKR analysts. Additionally, similar to EOCs, fusion centers also often have personnel with specialized expertise, including fire service, public health and/or emergency management and response. When discussing staff capabilities and needs/requirements, fusion centers and EOCs should discuss specialized expertise contained in their center and explore additional, potential interaction. Additionally, letters of agreement (LOA) or MOUs can assist in formalizing and implementing agreed upon duties. (See Step Two)

Managers also need to address whether staff members require security clearances in case classified information needs to be shared between the fusion center and EOC. Managers should identify staff members who need security clearance and work through the fusion center to request the clearances through DHS.

Training Resources

- Which training tools/programs are currently being used by the EOC and fusion center?
- What can be done to facilitate the cross-training of personnel?
  - Fusion center staff should be trained on NIMS, ICS and the operational procedures of the EOC.
  - EOC or relevant emergency management staff should be trained on fusion center and intelligence and information sharing protocols, such as:
    - Privacy and security policies;
    - Receiving/Handling classified and unclassified information;
    - Receiving/Handling criminal intelligence information in accordance with Title 28 Code of Federal Regulations (CFR) Part 23;
    - The protection of information privacy and other legal rights in the context of the information sharing environment[1]; and
    - Receiving/handling CIKR related information, such as protected critical infrastructure information (PCII), sensitive security information (SSI), chemical-terrorism vulnerability information (CVI) and/or safeguards information (SGI).

[1] Additional resources and training on privacy and civil liberties issues in the information sharing environment are available at http://www.it.ojp.gov/PrivacyLiberty and http://www.ise.gov/pages/privacy-overview.aspx.

- What training needs to be developed to fill in any gaps?
- Are exercises conducted between the centers to build relationships and interoperability? (See Step Four)
- Is the State exercise calendar being reviewed for opportunities to test anticipated interactions?

Available and Accessible Information

Before determining what information will be shared and how it will be shared, it is essential that EOCs describe what information they would like to receive from the fusion center and vice versa. To identify these needs/requirements, the fusion center and EOC should describe their current processes, capabilities and what products they develop and share. Once the current landscape is described, the respective centers can identify what information they would like to receive and how they would like to receive it. Additionally, knowing a customer's needs/requirements will help shape the products produced or identify gaps in information that the fusion center or EOC could fill with the creation of new products or reports.

The EOC and anyone receiving information from the fusion center must adhere to the fusion center privacy policy and dissemination policy, as applicable. Additionally, prior to receiving law enforcement or intelligence information, EOCs must develop and maintain a safeguarding policy to ensure this information is handled properly, not shared with media or public and destroyed properly. EOCs should address this by developing their own policy or plan, adopting the fusion centers security policy or plan or via an MOU with the fusion center.

Fusion Center Baseline Capabilities:

I. Fusion Process Capabilities:

D. Intelligence Analysis and Production

1. ***Analytic Products.*** *Fusion centers shall develop, implement and maintain a production plan that describes the types of analysis and products they intend to provide for their customers and partners, how often or in what circumstances the product will be produced and how each product type will be disseminated.*

   c. *Identify stakeholders and customer base for specific product lines and request feedback from customers to guide future products.*

   d. *Ensure the production of value-added intelligence products that support the development of performance-driven, risk-based prevention, protection, response and consequence management programs.*

Fusion centers produce a variety of products for their customers, including daily, weekly and/or monthly intelligence reports, special bulletins that describe threats or crime problems, crime trend reports, officer safety bulletins, be-on-the-lookout notices, tactical analytical reports and responses to requests for information (RFI). Unclassified reports specific to EOC operations and responsibilities should be shared with the EOC to improve its situational awareness and provide a common operating picture. The frequency of the reporting should be mutually agreed upon with the understanding that both parties should be involved in information sharing. These agreements may include how jurisdictions, law enforcement agencies and the public safety community communicate with fusion centers and EOCs, as well as how fusion centers communicate with the intelligence community. The issues that affect information sharing between the fusion center and EOC have several components—the first being the classification level of the information and the security classification levels held by the EOC participants.

Typically, most of the EOC personnel do not hold security clearances; therefore, the information briefed may be limited to UNCLASSIFIED or FOR OFFICIAL USE ONLY (FOUO). Providing a primer on classification would mitigate concerns of the EOC personnel regarding the types of information they may or may not receive. A second situation may involve an ongoing criminal investigation that would be compromised by wide dissemination or unauthorized or inadvertent disclosure. Additionally, any personnel, including those from an EOC, who may need information from or access to law enforcement databases need to be properly vetted to ensure compliance with access or 28 CFR Part 23 restrictions. 28 CFR Part 23 is a guideline for law enforcement agencies. This regulation contains implementing standards for operating Federally funded multijurisdictional criminal intelligence systems. It also provides guidance in the areas of submission and entry of criminal intelligence information, security, inquiry, dissemination and the review-and-purge process.

Critical Infrastructure represent assets, systems and networks, whether physical or virtual, so vital to a community and/or the United States that the incapacity or destruction of such assets, systems or networks would have a debilitating impact on the community's or the country's security, continuity of government, continuity of operations, public health, public consciousness or a combination of these effects.

Key Resources represent publicly or privately controlled resources essential to the minimal operations of the economy and government.

Ultimately, the fusion center will have to determine whether to distribute this type of information and the impact of any potential State, local or Federal laws and regulations, such as 28 CFR Part 23 restrictions.

Additionally, the fusion center may be a repository for CIKR information that can be shared with the EOC during an incident and also leveraged by the EOC to assist with applicable response and recovery efforts. As intelligence analysis and infrastructure protection programs grow and evolve, they will likely be housed in the fusion centers. This relationship strengthens the information sharing possibilities.

Continuity of Operations

Continuity of Operations (COOP) planning and capabilities may be an additional area of common interest. Most EOCs are equipped with backup power supplies, have alternate operating sites and rely on well-established plans. Emergency managers may be able to assist the fusion center with development of appropriate COOP plans, including identification or sharing of alternate sites and communications capabilities to continue the essential functions of the fusion centers. This coordination between the fusion center and EOC can also ensure they jointly leverage any backup resources, as well as provide mutual aid support should an incident or failure occur.

Fusion Center Baseline Capabilities:

II. Management and Administrative Capabilities:

E. Information Technology/Communications Infrastructure, Systems, Equipment, Facility and Physical Infrastructure

4. Contingency and Continuity-of-Operations Plans - Fusion centers shall have contingency and continuity-of-operations plans to ensure sustained execution of mission-critical processes and information technology systems during an event that causes these systems to fail and, if necessary, to ensure performance of essential functions at an alternate location during an emergency. (Guidelines 9, 10 and 18, Fusion Center Guidelines).

b. Develop the plans in coordination with emergency managers and other appropriate response and recovery officials.

c. Clearly define personnel roles and responsibilities during emergency situations.

Step Two: Establish Partnerships

Once leaders for the EOC and fusion center understand each other's capabilities, they should work together to establish agency-to-agency partnerships. Executive-level support for EOC/fusion center coordination or integration is essential. Some States have found it helpful to conduct meetings with the fusion center, law enforcement agency and emergency management agency directors to develop a uniform, cohesive response plan (including protocols for sharing information in response to an incident). Fusion centers will likely involve their governance board in this process. Regular interaction and relationship-building helps create a collaborative environment for the exchange of information. This concept is particularly true for States or jurisdictions with newly formed or less robust, fusion centers.

The EOC and fusion center should brief each other on policies, procedures and protocols. Meetings between EOC and fusion center leaders should be held at regular intervals to foster an ongoing understanding and appreciation of the roles, responsibilities and current endeavors undertaken by each center. Additionally, personnel management should consider the cross-training of personnel to ensure interagency familiarity with applicable processes and procedures (i.e., EOC staff on the handling of sensitive or classified information). This regular and routine interaction will help educate both entities and foster cooperation and is the most important element in developing a cooperative relationship.

Fusion Center Baseline Capabilities:

II. Management and Administrative Capabilities:

A. Management/Governance

1.b. The center's governance body should include representatives from the state and local law enforcement and public safety disciplines. This will enhance the center's ability to perform key baseline capabilities, including:

i.b. Supporting emergency management, response and recovery planning activities based on likely threat scenarios and at-risk targets.

Personnel exchanges, participation in (or creation of) liaison officer programs and development of working groups can help strengthen communication. Fusion center personnel who have also worked in an EOC will be better prepared to develop relationships with EOC staff members and anticipate EOC information requirements.

Once a partnership is established, MOUs, SOPs and/or CONOPS need to be formalized to document roles and responsibilities. MOUs should be drafted between the fusion center and the EOC coordinating agency. The purpose of such a document is to clarify the roles of each entity during EOC activation.

The Safeguard Iowa Partnership has developed a code of conduct manual to guide its liaisons serving in EOCs. The code of conduct manual helps to ensure that all liaisons understand their roles and responsibilities while at an EOC.

See Appendix E: Public-Private Partnerships: Safeguard Iowa Partnership's Code of Conduct Manual for Liaisons Serving at Emergency Operations Centers for more information.

In addition to this benefit, MOUs may also be used to resolve policy conflicts between parties. However, jurisdictions should be aware that obtaining the appropriate signatures on an MOU can be a time consuming and complicated process due in part to the number of parties who have to review and approve the document. Competing interests, State or local laws or organizational regulations and misunderstandings can either slow or stop the process. MOUs may be used as a means to resolve policy conflicts between parties.

Because an MOU can be extensive and define the overall relationship, as well as some of the details of the operation, all of the operational capabilities, roles and requirements may be addressed in the MOU. An example of an MOU is provided in Appendix B.

Step Three: Determine the Process

Information Exchange Procedures

Agreements should be developed describing what information and intelligence will be shared between the EOC and the fusion center, as well as how this data will be shared. When a fusion center releases information to an EOC, the intended recipients of the information should be clearly stated (taking security clearances into account), along with the intended purpose of the information. As discussed in Step One, EOCs should provide fusion centers with a list of personnel who can be contacted about sensitive and classified information. In turn, fusion centers should be prepared to share pertinent information with EOCs on such matters as disaster intelligence or criminal activities (in a format that does not present a conflict for EOC staff members without a security clearance).

Information exchange procedures between the EOC and fusion center should also take into account existing procedures for the exchange of information between the EOC, DHS and the law enforcement community. For example, if emergency managers already have procedures in place for communicating directly with the police, fire and sheriff's departments, how might that affect the information exchange process between the EOC and fusion center?

As fusion centers may provide direct representation in the EOC—either through a fusion center liaison, ESF-13—the EOC should use the fusion center as its conduit to communicate with and exchange information with the intelligence community. Intelligence and information should flow through the fusion center and then be sent to the EOC. Conversely, information and intelligence products, such as situation reports, incident action plans and long–range, plans should be distributed to the fusion center staff to indicate current and future priorities and concerns of the EOC. This way, fusion analysts can be aware of information needs or requirements that may be pertinent to the EOC.

Fusion Center Baseline Capabilities:

II. Management and Administrative Capabilities

A. Management/Governance

3. Collaborative Environment - Fusion centers shall identify the organizations that represent their core (permanent) and ad hoc stakeholders and the roles and responsibilities of each stakeholder and develop mechanisms and processes to facilitate a collaborative environment with these stakeholders. (Guidelines 4 and 5, Fusion Center Guidelines)

b. Include the identification of entities and individuals responsible for planning, developing and implementing prevention, protection, response and consequence-management efforts at the State, local and tribal levels.

f. Develop and implement a Memorandum of Understanding (MOU) or Agreement (MOA) and, if needed, nondisclosure agreements (NDA) between the center and each stakeholder who intends to participate in or partner with the fusion center.

The Fusion Liaison Officer (FLO) Program is a coordination of a network of fusion center liaison officers who are members of law enforcement, fire service, public health and other agencies (including public works, corrections and emergency management). This program has been established in several States to facilitate communication with fusion center stakeholders, including law enforcement and emergency management. FLOs coordinate information sharing activities among private-sector and CIKR partners, such as electric companies, oil refineries, banks and entertainment facilities. With the help of this network, fusion centers receive homeland security and crime-related information for assessment and analysis. Intelligence also flows from the national level and the fusion centers to field personnel via the network. The information flow to the field personnel provides the local government with the situational awareness information necessary to prevent, protect against or respond to events impacting their community.

One advantage of the fusion center is its ability to integrate information and intelligence from various law enforcement and homeland security agencies, as well as State and Federal entities, analyzing and disseminating pertinent information back to the jurisdiction. To avoid duplication or misunderstanding, the EOC should also channel any collected information to the fusion center, as appropriate and defined by the fusion center and EOC.

Fusion centers should ensure EOCs receive regular briefings at the appropriate classification level, along with their identified customers and stakeholders. Fusion centers can post open source information on computerized emergency management software, and there should be a clear understanding between EOCs and fusion centers about how often this information will be posted and updated. The updates can be posted after they are vetted by the fusion center personnel to ensure that sensitive information has not been added to the open source information and is not compromised. Using such portals will assist the EOC in its coordination and planning efforts.

Fusion Center Baseline Capabilities:

I. Fusion Process Capability

A. Planning and Requirements Development

8. ***Coordinate with Response and Recovery Officials.*** *Fusion Centers shall identify and coordinate with emergency managers and appropriate response and recovery personnel and operations centers to develop, implement and maintain a plan and procedures to ensure a common understanding of roles and responsibilities and to ensure intelligence and analysis capabilities can be leveraged to support emergency management operation activities, as appropriate, when events require such a response.*

   a. *Ensure that the center has identified its intelligence and analytical roles and responsibilities in accordance with the NIMS and ICS.*

Steady State versus Active State

EOC coordinators (as well as law enforcement and other homeland security officials) should be familiar with the operations of the fusion centers. EOC plans and protocols should include a trigger for activating (or partially activating) the EOC based on intelligence received from the fusion center.

Steady State: Steady state is the posture for routine, normal, day-to-day watch operations and situational awareness, contrasted by temporary periods of heightened alert or real-time response to threats or incidents.

Different information requirements are associated with a fusion center in a steady state versus an active state. On a daily basis, fusion centers should be prepared to provide information on potential events to the EOC coordinators. This is often done by including the emergency manager in the routine intelligence summaries (which are sometimes lengthy and have a small amount of relevant information buried inside). However, fusion centers should be prepared to send information that may be directly relevant to the jurisdiction and not assume that others will have the time to digest and recognize a potential threat to the jurisdiction. This activity would include notification of any activation of the fusion center to a higher level, which, in turn, would trigger the emergency manager to monitor the situation more closely and be prepared to activate (or partially activate) the EOC in a forward-leaning posture or in response to an incident.

During EOC activations, fusion centers may serve in a support function to the EOC and should plan to provide the EOC with intelligence briefings at agreed upon intervals or as needed and should provide additional information to the EOC director should the need arise between briefings. Classified information may be provided to the EOC director (if cleared), but the information can usually be provided to the EOC in an unclassified version for dissemination to the EOC general staff.

Actionable Intelligence

After agency-level partnerships have been established, it is important for fusion center and EOC leadership to identify to whom and under which circumstances actionable intelligence can be shared. If clear conditions are agreed upon, in advance, the exchange of appropriate information can occur in a timely fashion.

Actionable Intelligence

Intelligence should:

- Paint a picture;
- Tell a story;
- Guide the response; and
- Produce knowledge upon which a course of action can be developed/recommended for resolution.

Staffing

The fusion process may support EOC staff and emergency management planners by strengthening the information collection process of the EOC planning section. While the EOC and the fusion center leverage information that has been gathered, it is the primary responsibility of the fusion center to analyze the information and disseminate intelligence to the EOC.

Fusion center staffing varies widely from jurisdiction to jurisdiction and may include:

- Fusion center management;
- State, local, tribal, and/or territorial law enforcement;
- Intelligence analysts, crime analysts, GIS analysts/planners, CIKR analysts, etc.;
- Operational planners;
- IT support (may also support EOC IT);
- EOC directors or liaison;
- Federal liaisons;
- State or local terrorism liaison coordinators;
- Fire services;
- Emergency medical services (EMS);
- Public health; and
- Hazardous materials personnel.

The following steps may improve the integration and/or coordination of fusion center and EOC operations and exchange of information, but they may not be applicable in every jurisdiction.

- **Identification of Liaisons/Representatives:** There should be an identified liaison/representative between the fusion center and the EOC whose primary responsibility is to ensure coordination between the two entities. This may be a part-time or ancillary duty. The roles of this liaison/representative should be clearly documented and defined.
  - **ESF-13 (Public Safety and Security):** Consideration should be given to using fusion center personnel to staff the ESF-13 function during EOC activation. It will increase the ability of the fusion center to support the EOC with analytical capabilities and will provide reach-back capabilities to Federal, State and local intelligence resources.

- **Assignment of Full-time Analysts/Personnel:** Based on available resources, the EOC or responsible emergency management agency should consider assigning or detailing a full-time analyst to the fusion center. This analyst would have intimate knowledge of emergency management operations and serve as a subject matter expert (SME) on emergency management/response operations. The analyst's responsibilities would include providing SME support to fusion center operations and analysis and ensuring the timely and accurate flow of information between the fusion center and EOC before, during and after incidents. Additionally, a fusion center should consider assigning or placing an intelligence officer with appropriate clearances within the EOC during activation. This will ensure the continuous and vital flow of information and intelligence to the EOC, as well as reach-back for support from the fusion center.
- **Unification or Virtual Connection of Watch Offices/Desk:** The watch offices or duty desks of both the fusion center and EOC should consider virtually unifying to ensure that communication is exchanged in the most timely and accurate way possible. This would allow for the timely exchange, coordination and/or deconfliction of information while serving as a mechanism to formally integrate the fusion center's prevention efforts with the EOC's response efforts. This arrangement would also leverage finite resources/personnel.
- **Expansion of FLO Programs:** Existing FLO programs should be considered as a mechanism to enhance communication between the fusion center and the EOC, especially if dedicated analysts or liaisons responsible for this interaction have not been identified. Emergency management personnel should be considered for inclusion in the program, if they are not yet participating. If a FLO program does not yet exist, the fusion center should consider implementing it in order to build relationships with the EOC via multidisciplinary and SME personnel (e.g. fire services, EMS, emergency management and public health entities).

If fusion centers are co-located with the EOC, staffing may be shared with the EOC long-range planning sector, if the situation warrants. Additionally, fusion centers may be able to provide resources and support to the EOC, including sharing new technology as it becomes available, such as facial recognition tools.

Challenges

Arriving at a common understanding about what information to share and how to share it sometimes stands in the way of developing coordination between fusion centers and EOCs. Traditional models have not accounted for fusion centers and their increased ability to provide information and intelligence to the EOC. One way to address this challenge is through continuous efforts to familiarize the two entities with each other. Understanding of the chains of command, level of resource commitment and capabilities can only be achieved by training and exercising together. Developing common CONOPS and SOPs will also assist the coordination and communication even in the event of inevitable personnel changes.

Step Four: Training, Workshops and Exercises

One of the best ways to familiarize agencies with each other's staff is to jointly attend training and exercises. The sections below outline training and workshop resources.

Training

Training should be conducted to inform EOC members of the rules and regulations concerning classified information and the type of information they should expect to receive during briefings by the fusion center. A brief that describes the types of classified information, its origin and use can be offered to the EOC members in order to increase their understanding of what information they may or may not receive. Emphasis can be placed on how much information can be gleaned from open or unclassified sources.

Training courses that are applicable for EOC/emergency management and fusion center personnel include the following:

- *National Response Framework: IS-800.b.* This course introduces the guiding principles that all emergency and response partners need to prepare for and provide a unified response to all-hazards. The NRF "establishes a comprehensive, national, all-hazards approach to domestic incident response." http://training.fema.gov/EMIWeb/IS/IS800b.asp.
- *National Incident Management System: IS-700.a.* This course introduces NIMS by explaining its purpose, principles, key components and benefits. http://training.fema.gov/EMIWeb/IS/is700A.asp.
- *Incident Command System for Single Resources and Initial Action Incidents: IS-200.a.* This course is designed to enable personnel to operate efficiently during an incident or event within the ICS and provides training on and resources for personnel who are likely to assume a supervisory position within the ICS. http://training.fema.gov/EMIWeb/IS/IS200A.asp.
- *NIMS Multiagency Coordination System (MACS): IS-701a.* This course describes to participants the components of a MACS and how to establish relationships between all elements of the system. http://training.fema.gov/EMIWeb/IS/is701a.asp.
- *National Infrastructure Protection Plan (NIPP): IS-860a.* This course introduces the NIPP, identifies relevant authorities for CIKR protection efforts and related information-sharing processes. http://training.fema.gov/EMIWeb/IS/IS860a.asp.
- *Critical Infrastructure and Key Resources Support Annex: IS-821.* This course provides an introduction to the CIKR Support Annex to the NRF. http://training.fema.gov/EMIWeb/IS/IS821.asp.
- *Introduction to Incident Command System: IS-100.a.* This course introduces ICS and provides the foundation for higher level ICS training. This course describes the history, features and principles and organizational structure of ICS. It also explains the relationship between ICS and NIMS. http://training.fema.gov/EMIWeb/IS/IS100A.asp.
- *Introduction to ICS for Law Enforcement: IS-100.LEa.* This course introduces ICS and provides the foundation for higher-level ICS training. This course describes the history, features and principles and organizational structure of ICS. It also explains the relationship between ICS and the NIMS. This course uses the same objectives and content as other ICS 100 courses with law enforcement examples and exercises. http://training.fema.gov/EMIWeb/IS/IS100LEA.asp.
- *Public Safety and Security Annex: IS-813.* This course introduces the ESF-13 (Public Safety and Security) Annex. http://training.fema.gov/EMIWeb/IS/IS813.asp.
- *EOC Management and Operations: IS-775.* This course describes the role, design and functions of EOCs and their relationships as components of a MACS. The course contains disaster-related examples, activities and case studies that relate to EOC's and MACSs at the local, State and Federal levels of government. http://training.fema.gov/EMIWeb/IS/IS775.asp.

- *FEMA Integrated Emergency Management Course (IEMC).* IEMCs are four half-day exercise-based training courses that build awareness and skills needed to develop and implement policies, plans and procedures in an EOC. http://training.fema.gov/EMIWeb/IEMC/.
- *IEMC: EOC-Incident Management Team Interface: E947.* http://www.training.fema.gov/EMICourses/crsdetail.asp?cid=E947&ctype=R.
- *Federal Law Enforcement Training Center (FLETC) - Anti-Terrorism Intelligence Awareness Training Program (AIATP).* This course is an introductory awareness program designed to provide attendees with a working knowledge of the criminal intelligence process and applicable laws, guidelines, policies, tools and techniques. http://www.fletc.gov/state-and-local/tuition-free-training-programs/anti-terrorism-intelligence-awareness-training-program-aiatp.
- *FLETC - Introductory Intelligence Analyst Training Program (IIATP).* This course provides a historical, legal and ethical basis for law enforcement intelligence collection, retention and dissemination activities in accordance with the intelligence cycle. http://www.fletc.gov/state-and-local/tuition-free-training-programs/introductory-intelligence-analyst-training-program-iiatp.
- *Training Resources for State, Local and Tribal Fusion Centers on Privacy and Civil Liberties Issues in the Information Sharing Environment.* Training and resources, including privacy policy templates, for protecting information privacy and other legal rights and civil liberties issues in the context of the ISE are available at http://www.it.ojp.gov/PrivacyLiberty and http://www.ise.gov/pages/privacy-overview.aspx.
- *Training on 28 CFR Part 23.* 28 CFR Part 23 was issued to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information. It has been an important part of the intelligence landscape. This training is designed to help State and local representatives understand the guidelines that govern the development and implementation of policies and systems that facilitate intelligence sharing. Training includes overview of the regulation; compliance requirements; storage requirements; inquiry and dissemination requirements and review and purge requirements. The online training may be accessed through the secure National Criminal Intelligence Resource Center (NCIRC.) Web site, accessible through HSIN, LEO and RISS. http://www.iir.com/28cfr/Overview.htm.
- *Chemical-Terrorism Vulnerability Information Authorized User Training* is available online at http://www.dhs.gov/files/programs/gc_1181835547413.shtm.
- *Protected Critical Infrastructure Information Program Authorized User Training* is available online at https://pciims.dhs.gov/pciims.

Fusion Center Baseline Capabilities:

II. Management and Administrative Capabilities:

D. Personnel and Training

3. ***Training Plan.*** *Fusion centers shall develop and document a training plan to ensure that personnel and partners understand the intelligence process and fusion center's mission, functions, plans and procedures. The plan shall identify the basic training needs of all center personnel and identify specialized training needed to address the center's mission and current information requirements. (Guidelines 12 and 13, Fusion Center Guidelines)*

   b. *At a minimum, all center personnel should be trained on:*

      ii. *Roles and responsibilities of intelligence and analytical functions in accordance with NIMS and ICS.*

- *FLO Programs*. FLO Programs, as mentioned previously, facilitate the development and coordination of a network of FLOs who are members of local or State law enforcement, fire services, public health and other agencies, such as public works, corrections and emergency management. The network of FLOs ensures that vital disciplines participate in the fusion process and serve as the conduit through which homeland security and crime-related information flows to the fusion center for assessment and analysis. The FLO Program Technical Assistance is also offered through the joint DHS/DOJ Fusion Process Technical Assistance Program to assist in developing and implementing this program. Emergency management stakeholders are listed as potential partners in the program and are encouraged to participate.

Additional information on FLO programs is available via the *Establishing a Fusion Liaison Officer Program: A Guide and Workbook of Planning and Development Considerations* located on the LLIS System at www.llis.dhs.gov and NCIRC at www.ncirc.gov.

Workshops

Workshops should be held for fusion center and EOC staff (especially planning staff) to familiarize EOC staff with the capabilities of the fusion center and vice versa. The workshops should outline the concept of operations for how the EOC and fusion center will access each other's capabilities. In particular, workshops should include a discussion of databases and how they will be used and connected during activation of the EOC. Workshops can also be regularly scheduled to familiarize fusion center and EOC staff and to provide updates on tools, capabilities or other resources leveraged in the respective centers.

As part of the DHS/DOJ Fusion Process Technical Assistance Program, the Fusion Center Exchange Program supports the exchange of fusion center personnel and the associated exchange of operational best practices and lessons learned. The DHS/DOJ Fusion Process Technical Assistance facilitates interaction, information exchange activities and operations among directors and key intelligence and planning staff to solidify the national network of fusion centers.

The Fusion Process Technical Assistance Program also facilitates Fusion Center Direct Interaction Workshops, which allows SMEs to provide for efficient and effective sharing of best practices and lessons learned.

Exercises

Fusion Center Baseline Capabilities:

I. Fusion Process Capabilities:

A. Planning and Requirements Development

*10. **Exercises.** Fusion centers should conduct or participate in another agency's scenario-based tabletop and live training exercises to regularly assess their capabilities.*

b. Exercises should involve all relevant center personnel and constituents and should contribute to understanding the value of the statewide fusion process, the center's collection plan, the SAR process, analytical products, the center's role in the Information Sharing Environment and the center's role in response and recovery activities in accordance with NIMS and ICS.

Fusion centers and EOCs should consider regularly coordinating and/or conducting joint scenario-based tabletop and live training exercises to assess their communication capabilities and for the exchange of operational information identified in their SOPs and MOUs. These exercises should also be aimed at evaluating and deconflicting the roles and responsibilities of any identified personnel responsible for the coordination and/or integration of these efforts. The use of the exercise evaluation guides also provides a measurement tool for identifying gaps in training or roles and responsibilities and further ensures a level of NIMS compliance. The exercises should be Homeland Security Exercise and Evaluation Program (HSEEP) compliant.

The Terrorism Prevention Exercise Program (TPEP) conducts exercises and supports activities that increase awareness, coordination and information sharing among homeland security and law enforcement officials at all levels of government. The exercises assess prevention capabilities to include intelligence analysis, information sharing and recognition of indicators and warnings.

Case Studies and Examples

Fusion centers play a critical role in providing planning and operations intelligence support for special events of various sizes. As a central repository of strategic and tactical information, fusion centers provide law enforcement, public safety, emergency management and other partners with information and intelligence to guide preparations and support tactical decision-making during a special event. The planning, organizational structure and processes for collecting, analyzing, deconflicting and disseminating information can be scaled to meet operational needs and resource constraints.

In planning for special events, as well as National Special Security Events (NSSEs), jurisdictions will have to incorporate all four mission areas (prevent, protect, respond and recover) in the planning effort. As the fusion centers have grown and become more robust, they are able to collect information from a wide variety of sources and deliver finished analytical products that will help form decisions about resource allocations needed to address the event.

In prevention planning, the various information collectors attached to the fusion process (which includes the Federal, local, tribal, territorial, and private-sector authorities) should prepare a collection plan that focuses on the issues surrounding the event. The input can come from the Federal Intelligence Community, State and local law enforcement, other public sector entities, first responders and the community. The prevention planning effort will provide information to the event's stakeholders in the run up to the event and at the operations centers during the event.

The planning for the Republican and Democratic conventions, as well as the Presidential Inauguration, illustrate how prevention concepts and processes can be incorporated into the overall planning process. The jurisdiction in which the event will be held begins the prevention planning process many months before the event. The fusion center, which incorporates a variety of State, local, tribal, territorial, and Federal participants, can begin the process of collecting, analyzing and disseminating information and intelligence. The U.S. Secret Service (USSS) is the lead Federal agency for the NSSE and makes plans to protect either the candidates or the President and Vice President during the events. They are an integral part of the planning process since the primary effort is to prevent an attack on the individuals they are tasked to protect.

The fusion center analysts can use open source collection methods to assess the threat to the event. For example, they can gather information on groups that plan direct action against the event and grade the threat. This information can be passed to the command staff of the police department, FBI, USSS and other officials who can make decisions about resource utilization. It also allows them to make decisions about where to deploy resources to harden targets not previously considered.

Also important in the prevention planning effort is input from the DHS Protective Security Advisors who interface with the owners of the critical infrastructure and key resources potentially affected during the event. The owners of the CIKR can provide threat data as well as receive appropriately vetted material to protect their property.

In jurisdictions where the fusion center and the EOC are co-located, successful relationships are built on a series of steps that define the roles and responsibilities of the participants. The necessary components are enabling legislation, MOU between the parent agencies, SOPs and a genuine desire to exchange information. The watch offices in the EOC and fusion center have developed an information sharing protocol that encourages open communication.

The fusion center and EOC exchange analysts to ensure that the proper classification is applied to the information so that it can be appropriately disseminated.

The FLO Program can be used to enhance the relationship between the fusion center and the EOC. States have trained emergency management, first responder and other public sector, non-law enforcement personnel as liaison officers. The benefit of this program is that there is a strong communication channel between the fusion center and the liaison's parent agency. As more trained liaison officers are assigned to an EOC during activation, the bond between the fusion center and the EOC strengthens.

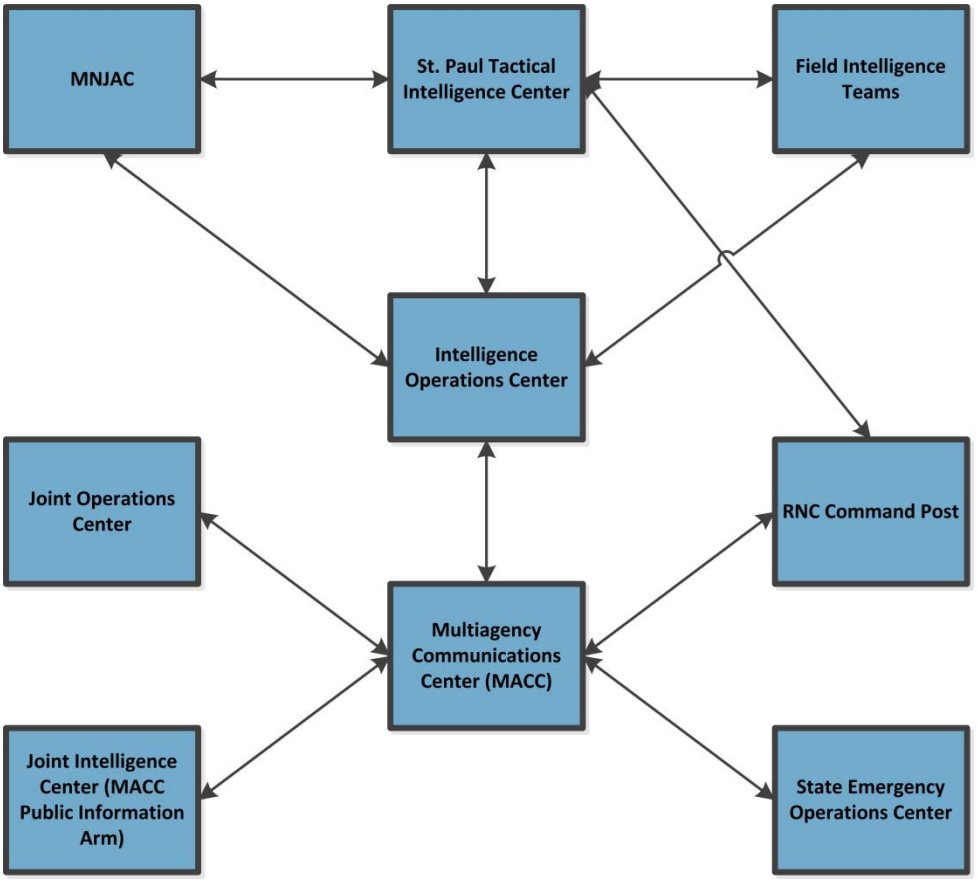
Minnesota Joint Analysis Center and the Republican National Convention

The Minnesota Joint Analysis Center (MNJAC), which is the State fusion center, provided critical information and intelligence support during the Republican National Convention (RNC) held in Minneapolis-Saint Paul, Minnesota, September 1–4, 2008. Because of the NSSE classification, the USSS was the lead agency, while the FBI, the Saint Paul Police Department and the MNJAC shared the responsibility for collecting, fusing, analyzing and disseminating all information in support of RNC security operations. Additional agencies assisting with event security included FEMA, U.S. Coast Guard, Customs and Border Protection, Transportation Security Administration, DHS I&A, Domestic Nuclear Detection Office, U.S. Immigration and Customs Enforcement, Saint Paul Public Works and the RNC Host Committee.

Approximately 45,000 delegates, alternate delegates, volunteers, members of the media and other guests traveled to the area. The RNC also drew a large number of protestors resulting in a public safety threat and a crowd control issue (law enforcement arrested 818 individuals). During the RNC, the MNJAC had personnel assigned to the Tactical Intelligence Center (TIC) and the intelligence operations center (IOC), which created an efficient flow of information to and from the centers. MNJAC staff also helped to maintain a current operational picture within the IOC.

MNJAC was able to utilize the Intelligence Communications Enterprise for Information Sharing and Exchange (ICEFISHX) network (which is used to collect information about suspicious activity relating to criminal activity and infrastructure protection in Minnesota) to broadcast quickly across State boundaries to the other fusion centers and Federal agencies. This allowed MNJAC to obtain background information and criminal records concerning individuals and groups participating in protest activity.

The following diagram[2] shows how information was shared between numerous stakeholders:



Throughout the RNC and for all accompanying activities, the collaboration and co-location of Federal, State and local agencies, as well as the private sector, provided a supportive environment, which resulted in timely exchange of information and successful management of multiple activities. Specifically, the MNJAC's capability to reach out to surrounding States, the Saint Paul Police Department's intelligence arm, the Minneapolis Police Department's intelligence unit and other Federal agencies provided significant strategic support during event planning phases, as well as during the event.

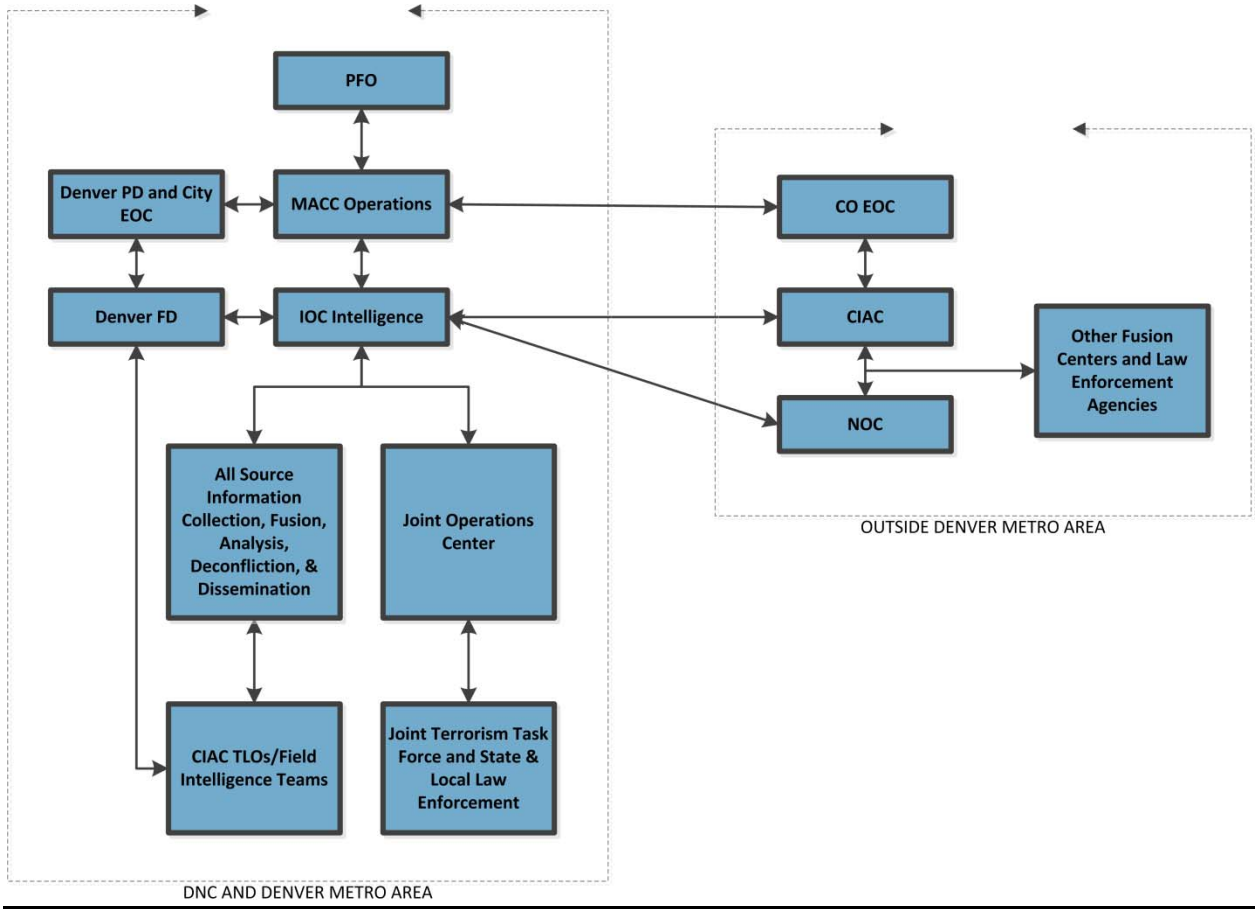
Colorado Intelligence Analysis Center and the 2008 Democratic National Convention

The Colorado Intelligence Analysis Center (CIAC) provided critical information and intelligence support during the Democratic National Convention (DNC) held in Denver, Colorado, August 25–28, 2008. The CIAC is a State fusion center located in a Denver suburb and managed by the Colorado State Patrol and co-located in the same building with the State EOC. The CIAC and the FBI shared equal management

[2] Source: Fusion Center Spotlight, DHS/DOJ Fusion Process Technical Assistance Program and Services 2008.

responsibility for the IOC, which was responsible for collecting, fusing, analyzing, deconflicting and disseminating all information in support of DNC security operations.
Prior to the DNC, regular training was not conducted between the fusion center and the EOC. In preparation for the DNC, the CIAC trained more than 200 TLOs from various disciplines, who either were assigned to different commands and control centers during activation or backfilled spots in the CIAC. By mutual agreement, the Denver Police Department was the primary EOC, although the State EOC was also activated but was in a standby mode during the event. The CIAC commander was assigned to the EOC and provided EOC leadership with situational awareness. The CIAC commander also monitored the information sent to the EOC to ensure that classified information was not compromised. The CIAC briefed the EOC personnel at shift changes on investigations and potential threats, which was valuable to EOC personnel and kept the communications channels open.

Information pertinent to DNC security operations within the Denver metropolitan area was coordinated by the IOC. The CIAC, along with the DHS National Operations Center (NOC) in Washington, D.C., coordinated information with fusion centers around the country and other State and local law enforcement agencies. The CIAC also acted as the conduit for intelligence and other information to the Colorado State EOC. The following diagram[3] shows the information flow between the various stakeholders:



[3] Source: Fusion Center Spotlight, DHS/DOJ Fusion Process Technical Assistance Program and Services 2008.

The CIAC was primarily responsible for activities outside the DNC area of operation, including coordinating with the NOC and other fusion centers. It supported some IOC activities. To provide the IOC with an intelligence collection capability, the CIAC overlaid the Field Intelligence Team (FIT) concept with its existing TLO program. Comprised of a team of multiagency TLOs, FITs were responsible for providing real-time intelligence and information about criminal and public safety incidents.

The DNC provides many examples of how a State or local fusion center can support the planning and execution of event security plans. The collaboration and co-location of Federal, State and local agencies provided a supportive environment which resulted in timely exchange of information and a successful management of multiple activities. The cooperation between the CIAC and the FBI in running the IOC provides a model for future NSSEs and other special events.

For More Information

Please see the *Fusion Center Spotlight - Supporting Special Events: Colorado Intelligence Analysis Center and the 2008 Democratic National Convention located in the Fusion Center and EOC Integration and Coordination Workshop: Reference Documents* kit for more information on the operations and interaction of the CIAC during the DNC. This document is also located on the LLIS System at www.llis.dhs.gov and the NCIRC at www.ncirc.gov.

This page intentionally left blank.

Appendix A: Glossary and Acronyms

Glossary

All-Crimes Approach

An approach that incorporates terrorism and other high-risk threats into the existing crime-fighting framework, to ensure that possible precursor crimes are screened and analyzed for linkages to larger-scale terrorist or other crimes. This approach recognizes that there is a nexus between types of criminal activity (e.g., illegal drug operations, gangs, money laundering, fraud, identity theft and terrorism). Using an all-crimes approach does not imply that a fusion center must address every single crime that occurs within their area of responsibility. Rather, the routine risk assessment that a fusion center develops or supports development of should assist in prioritizing which crimes and/or hazards a State or region should address and, in the development of a collection plan, identify which other sources of information may be useful for examining possible connections with other crimes.

All-Hazards Approach

An approach that refers to preparedness for terrorist attacks, major disasters and other emergencies within the United States. (Source: HSPD-8, December 17, 2003.) Within the context of the fusion process, some fusion centers have defined their mission to include an all-hazards approach. While the application of this approach varies, in general, it means that the fusion center has identified and prioritized types of major disasters and emergencies, beyond terrorism and crime, that could occur within their jurisdiction. The fusion center also gathers, analyzes and disseminates information which would assist the relevant responsible agencies (e.g., law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response or recovery efforts of those incidents. A fusion center can use an all-hazards approach but not address in its operations every possible hazard. Part of the annual risk assessment a fusion center develops or supports development of should identify which hazards a State or region should prioritize within its homeland security planning process, as well as provide the fusion center with the prioritization needed to develop relevant SINs.

Analysis

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.

Baseline Capability

A capability provides the means to accomplish a mission or function resulting from the performance of one or more critical tasks, under specified conditions, to target levels of performance. A capability may be delivered with any combination of properly planned, organized, equipped, trained and exercised personnel that achieves the desired outcome (Source: National Preparedness Guidelines, p. 40). Within the context of this document, a baseline capability for a fusion center is a capability necessary for the fusion center to perform its core functions of gathering, processing, analyzing and disseminating terrorism, homeland security and law enforcement information.

Classified Information/Intelligence

A uniform system for classifying, safeguarding and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is 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.

Collation (of Information)

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.

Collection (of Information)

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.

Collection Plan

The preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information and a timeline for collecting the information.

Coordination

The process of interrelating work functions, responsibilities, duties, resources and initiatives directed toward goal attainment.

Critical Infrastructure and Key Resource (CIKR)

Systems, assets and networks, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters. Key resources consists of any publicly or privately controlled resources essential to the minimal operations of the economy and government.

Dissemination (of Intelligence)

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.

Emergency Operations Center (EOC)

The physical location where the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement and medical services), by jurisdiction (e.g., Federal, State, regional, tribal, city, county), or some combination thereof.

Emergency Support Functions (ESF)

Used by the Federal Government and many State governments as the primary mechanism at the operational level to organize and provide assistance. ESFs align categories of resources and provide strategic objectives for their use. ESFs utilize standardized resource management concepts, such as typing, inventorying and tracking, to facilitate the dispatch, deployment and recovery of resources before, during and after an incident.

For Official Use Only (FOUO)

A designation previously used for marking unclassified sensitive information. This designation has been replaced by the Controlled Unclassified Information (CUI) Framework.

Fusion Center

A collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing the ability to detect, prevent, investigate and respond to criminal and terrorism activity (*Fusion Center Guidelines,* August 2006). Recognized as a valuable information sharing resource, State and major urban area fusion centers are the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information, homeland security information and law enforcement information related to terrorism.

Fusion Center Guidelines, August 2006

A nationally recognized document developed to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships and improved crime-fighting and anti-terrorism capabilities.

Fusion Process

The overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response and consequence management programs. The fusion process turns information and intelligence into actionable knowledge (*Fusion Center Guidelines,* August 2006).

Incident

An occurrence, natural or manmade, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies and other occurrences requiring an emergency response.

Incident Command

The ICS organizational element responsible for overall management of the incident and consisting of the Incident Commander (either single or unified command structure) and any assigned supporting staff.

Information

Pieces of raw, unanalyzed data that identify persons, evidence or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

Information Sharing Environment (ISE)

A trusted partnership among all levels of government, the private sector and foreign partners to detect, prevent, preempt and mitigate the effects of terrorism against territory, people and interests of the United States. This partnership enables the trusted, secure and appropriate exchange of terrorism information, in the first instance, across the five Federal communities; to and from State, local, tribal, and territorial governments, foreign allies and the private sector and at all levels of security classifications.

Information Sharing System

An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes and/or events in order to enhance prevention and apprehension activities by law enforcement.

Information System

An organized means, whether manual or electronic, of collecting, processing, storing and retrieving information on individual entities for purposes of record and reference.

Intelligence (Criminal)

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 (or investigate or prosecute).

Intelligence Analyst

A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution or arriving at an assessment of a crime problem or crime group.

Intelligence Community

The intelligence community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

Intelligence Cycle

Also known as fusion process. *See Fusion Process*.

Intelligence Function

That activity within a law enforcement agency responsible for some aspect of law enforcement intelligence, whether collection, analysis and/or dissemination.

Intelligence Process

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.

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 the prevention of crimes, target hardening, apprehension of offenders and prosecution.

Intelligence Records Guidelines

Derived from the Federal regulation 28 CFR Part 23, these are guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

Joint Terrorism Task Force (JTTF)

The joint operational group, led by the FBI, that leverages the collective resources of member agencies to prevent, investigate, disrupt and deter terrorism threats that affect United States interests and facilitate information sharing among partner agencies.

Law Enforcement Intelligence

The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems and criminal activity with the intent to pursue criminal prosecution or project crime trends or support informed decision making by management.

Law Enforcement Sensitive (LES)

Sensitive but unclassified information specifically compiled for law enforcement purposes that, if not protected from unauthorized access, could reasonably be expected to (1) interfere with law enforcement proceedings, (2) deprive a person of a right to a fair trial or impartial adjudication, (3) constitute an unwarranted invasion of the personal privacy of others, (4) disclose the identity of a confidential source, (5) disclose investigative techniques and procedures and/or 6) endanger the life or physical safety of an individual.

Multiagency Coordination System (MACS)

A system that provides the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration and information coordination. MACS assist agencies and organizations responding to an incident. The elements of a MACS include facilities, equipment, personnel, procedures and communications. Two of the most commonly used elements are EOCs and multiagency coordination groups.

National Incident Management System (NIMS)

A set of principles that provides a systematic, proactive approach guiding government agencies at all levels, nongovernmental organizations and the private sector to work seamlessly to prevent, protect against, respond to, recover from and mitigate the effects of incidents, regardless of cause, size, location or complexity, in order to reduce the loss of life or property and harm to the environment.

National Information Exchange Model (NIEM)

A joint technical and functional standards program initiated by DHS and DOJ that supports national-level interoperable information sharing.

National Intelligence or Intelligence Related to National Security

Defined by Section 3 of the National Security Act of 1947, as amended, as "A) information relating to the capabilities intentions or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (known as foreign intelligence); and B) "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (known as "counterintelligence"), regardless of the source from which derived and including information gathered within or outside the United States, that (A) pertains to more than one United States Government agency; and (B) involves (i) threats to the United States, its people, property, or interests'; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on the United States national or homeland security." (50 U.S.C. § 401a) The goal of the National Intelligence effort is to provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy and the protection of United States national interests from foreign security threats. (Executive Order 12333)

National Operations Center (NOC)

Serves as the primary national hub for situational awareness and operations coordination across the Federal Government for incident management. The NOC provides the Secretary of Homeland Security and other principals with information necessary to make critical national-level incident management decisions.

Network

A structure of interconnecting components designed to communicate with each other and perform a function or functions as a unit in a specified manner.

Office of Intelligence and Analysis (I&A)

I&A is a component of DHS and the national Intelligence Community (IC). It ensures that information related to homeland security threats is collected, analyzed and disseminated to the full spectrum of homeland security customers in DHS, at State, local, tribal, and territorial levels, in the private sector and in the IC.

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.

Policy

The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities which are directed toward the attainment of goals.

Privacy (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 in which the legal process permits use of the personally identifiable information.

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 the use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation.

Privacy Act

Legislation that allows an individual to review almost all Federal files pertaining to him/her, places restrictions on the disclosure of personally identifiable information, specifies that there be no secret records systems on individuals and compels the government to reveal its information sources.

Procedure

A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal-oriented. However, policies establish limits to action, whereas procedures direct responses within those limits.

Recommendations

Suggestions for actions to be taken based on the findings of an analysis.

Responsibility

Responsibility reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

Risk Assessment

Risk is defined as the product of three principal variables: 1) threat (the likelihood of an attack occurring), 2) vulnerability and 3) consequence (the relative exposure and expected impact of an attack). Risk assessment is the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability and consequence. A risk assessment may include scenarios in which two or more risks interact to create greater or lesser impact. A risk assessment provides the basis for the rank ordering of risks and for establishing priorities for countermeasures.

Risk is classically represented as the product of a probability of a particular outcome and the results of that outcome. A statewide or regional assessment of the threats, vulnerabilities and consequences faced by the fusion center's geographic area responsibility. The risk assessment is used to identify priority information requirements for the fusion center and to support State and urban area homeland security preparedness planning efforts to allocate funding, capabilities and other resources.
In traditional criminal intelligence, a risk assessment means an analysis of a target, illegal commodity or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

Security

A series of procedures and measures that, when combined, provide protection of people from harm, information from improper disclosure or alteration and assets from theft or damage (Criminal Justice Commission, 1995).

Situation Report (SitRep)

Document that contains confirmed or verified information and explicit details (who, what, where and how) relating to an incident.

Threat Assessment

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.

Unified Command (UC)

An ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior persons from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single incident action plan.

Urban Area Security Initiative (UASI)

UASI addresses the unique multi-disciplinary planning, operations, equipment, training and exercise needs of high-threat, high-density urban areas.

Warning

To notify in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack.

Acronyms

ACAMS	Automated Critical Asset Management System
AIATP	Anti-Terrorism Intelligence Awareness Training Program
BJA	Bureau of Justice Assistance
CFR	Code of Federal Regulations
CIAC	Colorado Intelligence Analysis Center
CICC	Criminal Intelligence Coordinating Council
CIKR	Critical Infrastructure and Key Resources
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CPG	Comprehensive Preparedness Guide
CVI	Chemical-Terrorism Vulnerability Information
DHS	Department of Homeland Security
DNC	Democratic National Convention
DOC	Department Operations Centers
DOJ	Department of Justice
EEIs	Essential Elements of Information
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
Epi-X	Epidemic Information Exchange
ESF	Emergency Support Functions
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FLO	Fusion Liaison Officer
FOUO	For Official Use Only
FPC	Federal Preparedness Coordinator
GIS	Geographic Information System
GIWG	Global Intelligence Working Group
Global	Global Justice Information Sharing Initiative
HAN	Health Alert Network
HSDN	Homeland Security Data Network
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IAP	Incident Action Plan
IC	Incident Command
ICP	Information Collection Plan
ICS	Incident Command System
IEMC	Integrated Emergency Management Course
IIATP	Introductory Intelligence Analyst Training Program
IOC	Intelligence Operations Center
IP	Office of Infrastructure Protection
ISE	Information Sharing Environment
IT	Information Technology
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online

LLIS	Lessons Learned Information Sharing
LOA	Letter of Agreement
MACS	Multiagency Coordination System
MNJAC	Minnesota Joint Analysis Center
MOU	Memorandum of Understanding
NCIRC	National Criminal Intelligence Resource Center
NEDSS	National Electronic Disease Surveillance System
NDA	Non-Disclosure Agreement
NIC	National Integration Center
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NPD	National Preparedness Directorate
NRCC	National Response Coordination Center
NRF	National Response Framework
NSSE	National Special Security Event
ODNI	Office of the Director of National Intelligence
OHA	Office of Health Affairs
PCII	Protected Critical Infrastructure Information
PM-ISE	Program Manager for the Information Sharing Environment
RFI	Request for information
RISS	Regional Information Sharing Systems
RNC	Republican National Convention
RRCC	Regional Response Coordination Center
SGI	Safeguards Information
SINs	Standing Information Needs
SME	Subject Matter Expert
SOP	Standard Operating Procedures
SSI	Sensitive Security Information
TCL	Target Capabilities List
TPEP	Terrorism Prevention Exercise Program
UASI	Urban Area Security Initiative
UC	Unified Command
USSS	United States Secret Service
WMD	Weapons of Mass Destruction

Appendix B: Draft Memorandum of Understanding

This draft MOU is provided only as a guide to describe how the fusion center and the EOC could interface. It is not intended as an MOU to establish a fusion center or an EOC. Guidance on an MOU to operate the fusion center is available at www.iir.com/global/resourcesGuidelines.htm.

Co-location or joint operations of the fusion center and the EOC is not done in every State; therefore, distinctions between co-located operations and separate operations will be addressed in this draft. In some cases, the centers may operate as a fusion center with combined staff or as a separate secure watch facility with fusion and EOC roles.

Some parts of this draft may not apply to your jurisdiction. Your jurisdiction may need to add additional language to clarify issues, relationships or to obtain signatures. It is not intended to be all inclusive but, rather, is provided as an example for fusion centers and EOCs to begin the process of developing an MOU appropriate for their situation and jurisdiction.

Draft Memorandum of Understanding

Between _____State Fusion Center and _____State Emergency Management Agency

I. Purpose

(In this section, clearly state the purpose of this MOU. Indicate that it is only to define how the two already established centers will interface to share information for the betterment of the State and the nation.)

The purpose of this memorandum of understanding (MOU) is to establish the policies that govern the activities of the agencies participating in interaction between the _____ Fusion Center and the _____Emergency Operations Center (EOC). The guidelines established herein will serve to maximize cooperation and to create a formal, effective working group capable of addressing the effective and efficient management, classification and dissemination of criminal, homeland security and/or terrorism-related threat and/or hazard information in the State of _____ and the United States of America.

II. Mission

(This section should include the mission statement of the fusion center and the EOC, with short concise and clear statement of the purpose and roles of the centers.)

This agreement reflects a collaborative effort between the _____ Fusion Center and _____ Emergency Management Agency to share strategic, operational and/or tactical homeland security, terrorism and/or criminal information and intelligence in support of emergency management, response and/or recovery operations—specifically information that has been deemed essential to support activities of EOCs before, during and after EOC activation for an incident, in accordance with essential information needs outlined below. *(If the specific types of information that will be shared have been identified, it can be described below or in an attachment).*

III. Governance

(Insert the composition of the Advisory Board. Consider the board composition to include the Head of the State Law Enforcement or Homeland Security Agency as the Chair, the State Coordinator of Emergency Management (Co-Chair), representatives from the Governor's Office or Agency/Office of Homeland Security or Preparedness, representative(s) from the legislative branch, a representative from the Federal Bureau of Investigation, a representative from the State National Guard, a representative from the Chief's associations representing police, fire, sheriff and a representative from State's fire programs and any other organizations deemed appropriate to have a stake in the Fusion Center and EOC interface process. Also consider how these members will be selected, appointed and replaced.)

The (Head of State Law Enforcement or Homeland Security Agency) shall be responsible for the operation of the Fusion Center. However, a multi-disciplined Governance/Advisory Board chaired by (Head of State Law Enforcement or Homeland Security Agency) or his/her designee will be tasked with reviewing operational processes and the effective and efficient information management systems and sharing of information statewide, to include the exchange of information between the fusion center and the EOC.

The Advisory Board will make recommendations to the Chair regarding the development of policy, resolution of conflicts and ensuring compliance with the MOU. The Advisory Board will also review reports submitted by any Fusion Center Working Groups and make annual reports to the Governor.

A multi-disciplined Fusion Center Working Group shall be established to make recommendations to the Advisory Board. The Working Group will be co-chaired by both Fusion Center and EOC onsite supervisors to report operational problems, enhancements and needs on a monthly basis to the Advisory Board along with a monthly activity report.

IV. Organization Structure

(This section will begin to define the global organizational and management structures. Keep in mind the purpose of the MOU is to get the decision makers to agree and commit to the global working relations. Some details concerning specific operations may be better suited for the Operations Manual or standard operating procedure (SOP) document.),

A. The fusion center consists of a combination of supervisors and analysts from each participating agency. The Fusion Center hosts representatives from the (State) EOC and other partners on a full or part-time basis depending on threat level and crisis management situations.

The Fusion Center consists of two separate functions: 1) the Watch Unit and 2) the Analytical Section composed of the (State) *Counterterrorism Unit* and the *Homeland Security Information and Intelligence Unit*. The Watch Unit will be staffed with members specifically trained and charged with receiving, processing and disseminating information, as well as requests for information (RFIs). The Analysis section will focus on the integration and analysis of intelligence information and will prepare reports, products and briefs. The (agencies/entities) will manage information systems and equipment for the State EOC and the Fusion Center, respectively.

Reports, products and information that match or meet pre-determined information needs of the EOC will be provided to the EOC watch center as a normal course of fusion center business during the EOC's steady state of operations.

When requested in support of an EOC activation or an incident (active state), the separate functions of the fusion center shall provide additional support:

1. Watch Unit will receive EOC situation reports and provide input to briefings, reports and presentations as needed. The information provided will assist in providing EOC and (State decision makers) with a more complete situational awareness.

2. Analysis Section will add EOC situation reports to the overall situational analysis. Analysts will augment the EOC staff as part of Emergency Support Function (ESF) 13 (Law Enforcement) and may augment other ESFs or EOC operations as requested (e.g., transportation, energy, public health). Depending on the circumstances, this augmentation may be a buildup of additional analytical support within the fusion center, or it may require analysts to relocate to the EOC with appropriate reach back capability to the fusion center. The final decision on the amount of resources to augment the EOC during an active state will rest with the fusion center. This will take into account all fusion center activities at and during the time of the EOC's activation.

B. The EOC consists of a dedicated staff to operate, maintain overall statewide situational awareness and be prepared to activate additional statewide resources to meet any support requirements of prevention, response, recovery or mitigation of any emergency. The EOC is operated by the (___) State Emergency Management Agency. Full-time staff may include personnel from other agencies to provide a constant statewide operational picture. A watch center will be maintained to receive and disseminate emergency information to decision makers, staff and supporting agencies.

1. Watch center will provide information to the fusion center to ensure both centers have a full operational picture at all times and advise the fusion center of any additional information requirements that result from a shift from the steady state to the active state. The watch center will also advise the fusion center when the EOC activates and make a recommendation regarding the extent the fusion center needs to augment the EOC.

2. EOC sections, when activated, will communicate information needs with the fusion center through the EOC watch center. If fusion center augmentation is requested and received, direct communication between the EOC command or sections and the fusion center analysis section is encouraged. All situation reports developed in the EOC will be provided to both the fusion center watch unit and the analysis unit. Fusion center analysis may be added to the situation reports, briefings and presentations in or for the EOC as appropriate for the classification of the documents. The EOC will follow all fusion center classification markings and security protocols. *(If the specific security protocols have been agreed upon, they can be described below or in an attachment)*

The EOC should be prepared to provide an appropriate working area for fusion center staff to operate when augmentation requires relocating fusion center resources to the EOC.

This may include access to secure spaces, access to secure communications, including telephone and/or email and access to secure storage containers to maintain secure documents.

C. Supervision

(This section should define the chain of command for supervisors and personnel.)

Keep in mind, the EOC, when activated, may use State agency personnel from many disciplines, outside resources and the private sector. An MOU between the fusion center and the EOC should be crafted in such a way as to outline the overall interaction between the two centers, without establishing a precedent that each agency will require specific agreements to staff the EOC.

The MOU should focus on how the two centers share information during a steady state and an active state to meet both centers operational requirements and expectations of the decision makers.

The fusion center manager reports to the (e.g., State Police Division Commander) who, through channels reports to the (Head of State Law Enforcement or Homeland Security Agency), to the Cabinet level position overseeing Public Safety and/or Law Enforcement and the Governor. The Designated Emergency Management Official assigned to the fusion center reports to the State Emergency Management Operations Division Director,

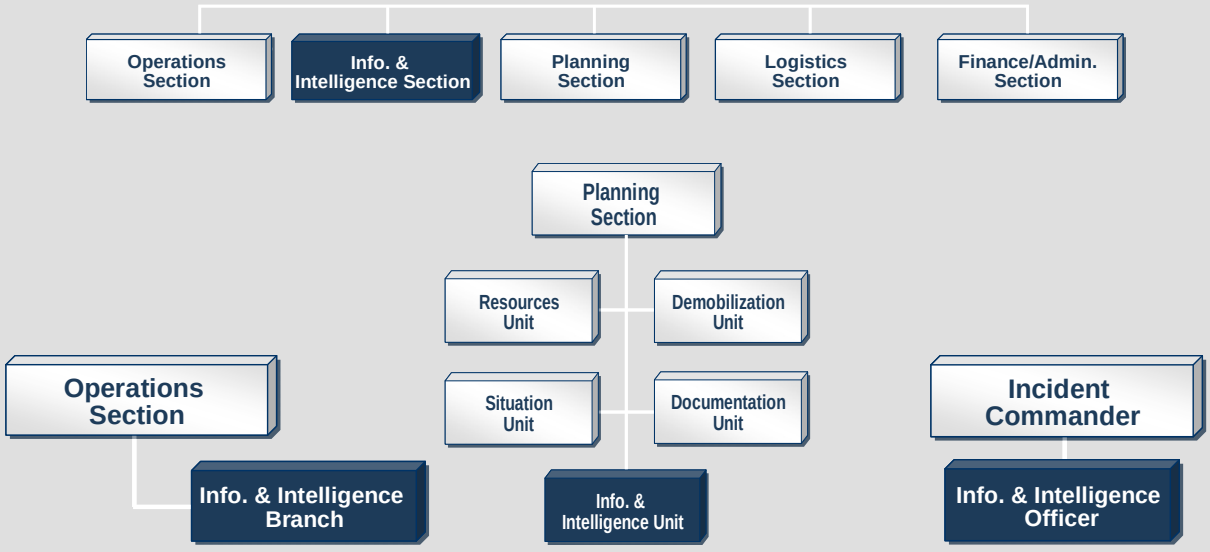
who through channels reports to the State Coordinator of Emergency Management, to the Cabinet-level position overseeing Public Safety and/or Emergency Management and the Governor.

During activation of the EOC, fusion center resources used to augment the EOC will continue to operate within their chain of command when located within the fusion center. If EOC augmentation requires fusion center personnel to be relocated to the EOC, they shall report to and operate under the EOC structure established. This shall be no different than any other EOC resource operating in the EOC during activation.

Problems and difficulties that may arise during any operation will be mutually addressed to the respective agency supervisors and resolved as expeditiously as possible. It is agreed that resolution of any and all problems at the lowest possible administrative level are in the best interest of the all parties.

An organization chart outlining where fusion center personnel will be assigned during an EOC activation may help to clarify lines of authority.

Based on the incident needs, the information and intelligence function may be activated as a fifth Section, as an element within the Operations or Planning Sections or as part of the Command Staff.



D. Personnel

(This section outlines the personnel resource commitment to support the EOC during steady state and active state. Inclusion of the minimum and if possible maximum, number of personnel to be assigned from a fusion center (and where they would report) will assist in accommodating the EOC's needs.)

The fusion center agrees to assign at least one supervisor and one analyst to augment the activation of the EOC. Initial augmentation will be at the fusion center. The supervisor will discuss the EOC's augmentation recommendations with on-duty fusion center staff, taking into account other operational requirements and available resources. If the EOC recommends onsite augmentation, the fusion center supervisor will determine the level of

support requested and verify which EOC organizational element the fusion center resources will be supporting.

(The following is an example of a staffing table which can be adjusted, as needed, based on the status of the EOC and the fusion centers operations.)

EOC Area	At Fusion Center	At EOC
Intelligence Officer	1 Analyst	1 Supervisory-Level Intelligence Officer
Intelligence/Information Section	1 Supervisor 1 Analyst	1 Section Chief 1 Supervisor 3 Analysts 1 Administrative
Operations Section: Intelligence/ Information Branch	1 Supervisor 1 Analyst	1 Branch Director 3 Analysts
Planning Section: Intelligence/ Information	1 Supervisor 1 Analyst	1 Team Leader 3 Analysts
ESF-13 Support	1 Supervisor	1 Analyst

E. Security Clearances and Classifications of Documents

(This section defines who has/can be granted security clearances based on sponsoring Federal agency requirements and the agreement to follow the fusion center or originator classification of documents.)

(Identified/All) members of the Fusion Center, regardless of their sponsoring agency, are required to have a SECRET (or higher) security clearance issued by a sponsoring Federal agency for access to national security classified information. Additionally, all members are required to have a (State Law Enforcement Police) background check. Personnel who do not have the appropriate clearances will be required to undergo a background investigation conducted by the Federal Bureau of Investigation (FBI) and/or the participating agency. All signatories agree to abide by originator controlled documents and third party dissemination regulations

EOC staff, including the State Coordinator, Deputy State Coordinators, Operations Section Chiefs, are required to have a SECRET (or higher) security clearance. Planning Section Chiefs and watch center supervisors are required to have a SECRET clearance issued by a sponsoring Federal agency for access to national security classified information.

V. Records and Reports

(This section will provide an overall understanding of the records, retention, reports and products of the fusion center. Again, it is important to keep in mind that the purpose of the MOU is not to document the details but the broad, overarching elements from which operations managers can work.)

In order to achieve uniformity and consistency among the participating agencies, it is agreed that incoming information received at the fusion center will be captured and documented in accordance with existing protocols currently in use by or formulated by the fusion center. Where

original information is developed that is allowed to be disseminated according to the existing protocols within the law enforcement, homeland security and intelligence communities, the fusion center will coordinate such dissemination.

All classified information received or generated by the fusion center and/or the EOC shall be controlled solely in accordance with existing United States government policy on the classification and handling of classified information. The Fusion Center Working Group may establish policy and recommend to the Governance and/or Advisory Board a need for the duplication of reports on participating agency forms, accessibility of information during EOC activations and securing of documents at the EOC during an active state.

Access to and use of these records will be in accordance with the Federal, State and local laws and the policies and procedures of the fusion center and/or the EOC. All (State Law Enforcement Agency) records and usage of same will be in accordance with Federal law, Department of Justice (DOJ) regulations, Title 28 Code of Federal Regulations (CFR) Part 23 and the agency regulations and policy, including but not limited to the (State Freedom of Information and Privacy Acts).

The Secure Room located at the fusion center is a FBI/DHS-certified facility for handling national security classified information and systems up to and including the (SECRET/TOP SECRET) level for the fusion center. As such, the information received, stored and managed within that facility will be handled in accordance with (FBI/DHS) requirements. Information related to the State EOC will be provided to the EOC for appropriate handling under established EOC protocols. The recorded schedule of events (meetings, operations, systems tests, etc.) shall be the responsibility of the Fusion Center Administrative Assistant.

A secure conference room will be maintained at the State EOC. This room will be secured in a manner to provide for work, discussions, briefings, video teleconferences, temporary storage of classified information up to the SECRET level. Fusion center augmented resources onsite at the EOC will have access to this space for working with or discussing classified information. Communication links with the fusion center capable of passing classified information between the centers will be available within this secure conference room.

VI. VI. Physical Location and Access

(This section provides the physical location of the fusion center, the EOC or a joint center. It addresses basic access to information, records or the centers themselves. Because the volume of information and classification of documents in the fusion center is generally going to be more stringent than that of the EOC, more focus may be placed on access to the fusion center. This focus should help assure the fusion center is cooperating with non-law enforcement agency partners, while maintaining the appropriate level of security for staff, facilities and products.)

If entities are not co-located, indicate separate locations and means of communications used to pass information during steady state and active state of EOC operations.

If they jointly operate a secure watch room as a means to coordinate information, indicate where this will occur.

The fusion center is located at (insert location and address; consider adding latitude/longitude coordinates as well). The EOC is located at (insert location and address; consider adding latitude/longitude coordinates as well).

To ensure awareness of all fusion center operations, the senior EOC officials will be briefed upon request and will be authorized access to appropriate fusion center records, subject to any pertinent legal and/or restriction of access. The senior EOC officials and their representatives can contact the fusion center directly at any time to receive investigative/threat updates and to request or provide information. Likewise, the EOC stands ready to provide appropriate briefings and access to fusion center staff or other officials as necessary.

VII. News Media and the Press

(In this section, provide an agreement on the release of information to the media. During an EOC activation, the Joint Information Center (JIC) will likely manage the public information dissemination. An agreement here is simply to articulate who has the lead in other cases.)

All media releases will be mutually agreed upon and jointly handled consistent with existing participating agency guidelines. Fusion center releases must have the prior approval of the (Head of State Law Enforcement or Homeland Security Agency) when the EOC is in the steady state. During EOC active state, all media releases will be handled by the Joint Information Center (JIC). Information gleaned from fusion center documents or reports should be cleared with the fusion center, fusion center representative or liaison working at the EOC before it is included in media releases.

VIII. Amendment of Agreement

(This section provides the tool to make changes to the MOU once the initial agreement is completed and signed. It may also provide the timeline for reviewing or redrafting the MOU.)

This agreement may only be amended by the mutual consent of the participating agencies or by a subsequent MOU. The addition of new participating agencies to either center will not be considered a formal change to the MOU and therefore, will not require approval of each current member; however, new members to either center must comply with this MOU as a condition of participating in either the fusion center or the EOC. Upon termination of the understanding or withdrawal from the center, all equipment will be returned to the supplying agency.

IX. Salaries and Compensation

(This section, if necessary, provides the language to identify which agency is responsible for joint center personnel costs. It also clarifies costs that would be included in any requests for reimbursement under the Stafford Act in accordance with a presidentially declared disaster. This language will vary depending how the center is funded.)

Salaries and allowable overtime of fusion center or EOC members will be paid by their respective agencies. Costs associated with EOC active state will be recorded and reported in accordance with EOC-established procedures to maximize the State's documentation of disaster-related expenses and to assist in documenting eligible reimbursable expenses when Federal assistance is authorized.

X. Discipline and Security

(This section provides the overall guidelines for the operations of the fusion center. Keeping in mind the purpose of the MOU, this section may be global with references to the specific Concept of Operations or Operations Manual for details. This section is designed to provide the decision makers with approval for the development of the operations documents created by the operations managers. It is not intended as the only documentation for fusion center operations guidelines.)

Both centers' personnel, regardless of the sponsoring agency, will be managed and guided by the SOPs, including the Security Policy and Classification and Dissemination Schedule. In addition to any standards of conduct policy directing (State Emergency Management) personnel or any other fusion center participating agency, all center personnel will be subject to the (State Law Enforcement or Homeland Security Agency) internal investigations for any action or conduct affecting the security of the fusion center or the State EOC. Security breaches will be subject to an internal (State Law Enforcement or Homeland Security Agency) investigation or that of a sponsoring Federal agency. Removal from the centers and/or elimination of access will be in accordance with the SOPs or policy established by the Fusion Center Working Group.

XI. Facilities Management and Access

(This section provides the overall responsibility for facility management and security. It may recognize that agency personnel outside of the State Law Enforcement or Homeland Security Agency will have controlled but limited access to the fusion center. Likewise, access to the EOC may be addressed here but should not confuse the EOCs accessibility for all participants in the EOC. Keep in mind, not everyone in the EOC has access to the fusion center, but, as a less secure facility, access to the EOC may be granted to fusion center staff, particularly when they are co-located.)

The fusion center facility will be managed by (State Law Enforcement or Homeland Security Agency) as agreed upon between, including overall facility security. The EOC facility will be managed by the State Emergency Management Agency. ID/Access cards and access control will be the responsibility of each center. Joint ID/Access cards should be used to provide access to both centers for individuals who are mutually agreed upon to have a need for such access. Sufficient emergency management staff with Federal security clearance and who have completed the necessary background investigations will have appropriate access to the secure room and systems, as granted by respective Federal agencies, located at the fusion center to conduct operations and perform system tests. Any telecommunications circuits to support emergency management systems (e.g., Homeland Security Information Network, Secure Video and Critical Infrastructure Warning Information Network connections), such as voice and facsimile circuits will remain the responsibility of the (State Emergency Management Agency) for maintenance and costs. Likewise, similar (State Law Enforcement or Homeland Security Agency) circuits, etc. will remain the responsibility of the (State Law Enforcement or Homeland Security Agency).

XII. Civil Liability and Indemnification

(This section should include the legal language determined necessary by the partnering parties to the MOU to cover the civil liability and indemnification for acts and omissions of personnel.)

Under no circumstances shall a participating agency assume liability for the actions of the centers' personnel who are not employed by that agency. Participating agencies shall not seek or be entitled to indemnification from any other participating agencies for any judgments, costs of litigation arising from the acts of the centers' personnel employed by that agency.

Each participating agency agrees to protect, indemnify and hold harmless all other participating agencies and their respective officers, agents and employees from and against all claims, actions and suits and will defend all other participating agencies and their respective officers, agents and employees, at its own cost and at no cost to the other participating agencies, in any suit, action or claim, including appeals for personal injury to or death of any person or loss or damage to property arising from or resulting from the activities or omissions of the said participating agencies under this agreement. These indemnification provisions are for the protection of the participating agencies and their respective officers, agents and employees and shall not establish,

of themselves, any liability to third parties. The provisions of this section shall survive the termination of this agreement.

XIII. Duration

(This section may provide the timeline which the parties have determined for reviewing the MOU or when it will be reviewed in its entirety. It could be included or combined with the section above regarding amendment of the agreement.)

This agreement will become effective upon the date the last of the undersigned participating agency representatives executes the agreement by affixing his/her signature. This will remain in effect until such time as the either center is disbanded. Disbanded does not refer to deactivation of the EOC following an incident. This MOU is intended to be indefinite. Participating agencies may withdraw their participation at any time after a sixty-day notice to all signatories of this document.

Note: A separate section above may be devoted to communication issues or it may be covered by operational guidelines.

Appendix C: Fusion Center and EOC Interface: Analysis of Coordination and Integration Best Practices

DHS/DOJ Fusion Process Technical Assistance Program and Services

United States Department of Justice

FUSION CENTER AND EMERGENCY OPERATIONS CENTER INTERFACE

Analysis of Coordination and Integration Best Practices

Overview

The joint Department of Homeland Security (DHS) and Department of Justice (DOJ) Fusion Process Technical Assistance Program supports the exchange of operational best practices and lessons learned to solidify the national network of fusion centers. In support of this initiative, the Fusion Process Technical Assistance Program examined the relationship between fusion centers and Emergency Operations Centers (EOCs) to determine how the two entities mutually support each other.

The objectives of this effort were to:

1. Determine each entity's capabilities and tools and how they are leveraged;
2. Identify ways those capabilities could be better incorporated or coordinated; and,
3. Identify which resources, training, and technical assistance could support the coordination and/or integration efforts between the two entities.

The following sites were visited: the Arizona Counter Terrorism Information Center (ACTIC), the Colorado Information Analysis Center (CIAC), the Florida Fusion Center (FFC), the Georgia Information Sharing and Analysis Center (GISAC), the Indiana Intelligence Fusion Center (IIFC), the Louisiana State Analytical & Fusion Exchange (LA-SAFE), the Michigan Intelligence Operations Center (MIOC), and the Virginia Fusion Center (VFC).

Each visit included discussions with fusion center and EOC personnel, including representatives from law enforcement, fire, emergency medical services (EMS), and emergency management disciplines. The following questions were posed during each visit:

- Is there a formal agreement that details how the two entities will interact?
- What systems or protocols facilitate communication between the two entities?
- Has there been any cross-training or have exercises been conducted to build relationships?
- If the two are co-located, is that arrangement beneficial to information sharing?
- If the two are not co-located, how do the entities communicate and share information?
- What types of information are shared by the two entities?
- How can the relationship between the fusion center and EOC be enhanced?

Arizona Counter Terrorism Information Center

The ACTIC, which is staffed by over 200 people, is a cross-jurisdictional partnership managed by the Arizona Department of Public Safety (DPS) and the Federal Bureau of Investigation (FBI). The center integrates Federal, State, and local law enforcement as well as first responders and emergency management. A Watch Center is the central location for information coming in and out of the ACTIC, and a governance board led by the Arizona DPS oversees its operations, which includes a robust Terrorism Liaison Officer (TLO) program. The TLO program, created to address an all-hazards environment, has progressively been embedded in all of the prevention, protection, response, and recovery activities in Arizona.

The EOCs throughout Arizona, whether at the State, local or county levels, are supported by the TLO program when they are activated during an incident. The examination of this interaction focused on the Arizona State EOC and interviews were conducted with ACTIC personnel, emergency managers, first responders, and law enforcement personnel from the City of Phoenix and Maricopa County.

The Arizona State EOC is overseen by the Arizona Department of Emergency Management and is not co-located with the ACTIC. The TLOs thought that their participation was valuable during EOC activation. In such situations, the ACTIC makes all of its unclassified information available to the EOC – an arrangement that enables the TLOs to access various fusion center databases and analytical resources such as e-Team and the State law enforcement system. These resources also include record checks from databases, geospatial analysis, Department of Motor Vehicle photographs, and tactical analytical products.

TLOs, which are drawn from the law enforcement, fire, EMS, public health and emergency management disciplines, are required to sign a non-disclosure agreement to assist in ensuring the protection of civil rights, civil liberties and privacy. Emergency management officials stated that the presence of a TLO in their EOC gave them access to appropriate data accumulated by the ACTIC, which mitigated the need to be co-located with the fusion center and enhanced their ability to respond to any situation. The ACTIC is currently developing Standard Operating Procedures (SOPs) that will guide how TLOs interact with Arizona's EOCs during an incident. Those SOPs will be maintained by the ACTIC and shared with its partners.

The ACTIC's outreach and training programs, as well as robust analytical and investigative capabilities, have enhanced the relationship between the fusion center and its public and private-sector partners.[1] Additionally, the ACTIC frequently conducts exercises and training with the State and local EOCs, and participated in the National Level Exercise (NLE) 2008, also known as TOPOFF, which offered the State's entire public safety community exercise and training opportunities.

Colorado Information Analysis Center

The relationship between the CIAC and the Colorado State EOC was examined during the Democratic National Convention (DNC) held in August 2008. While the CIAC and the State EOC are co-located in the same building, the communication between them has been episodic due to the evolution of their respective roles and responsibilities.

[1] Additional information on the ACTIC and its TLO Program is located on the Lessons Learned Information Sharing (LLIS) System at www.llis.dhs.gov.

The EOC staffs a watch officer 24/7 who serves as the link between the EOC and the CIAC. The EOC watch office receives CIAC products, such as daily/weekly reports and any special bulletins, while the CIAC periodically receives reports and briefings from the EOC watch office.

In preparation for that event, the CIAC trained more than 200 TLOs, including law enforcement, fire, EMS, emergency management, public health, agriculture, transportation, and military personnel. Some of those personnel were assigned to the various command centers activated during the DNC, and emergency management personnel continue to participate in the TLO program and receive the same training as law enforcement TLOs.

The DNC was a unique and challenging event for both the CIAC and the EOC. The Denver Police Department's EOC was the primary for the event, per mutual agreement. The State EOC was responsible for any emergency requirement outside of the City and County of Denver. The State EOC provided support to agencies participating in the management of the DNC that were not contracted by the Denver EOC or DNC management. The State of Colorado had several large events running concurrently with the DNC (The Colorado State Fair, The Taste of Colorado and Country Jam). These events require assistance and monitoring of the State EOC. The CIAC provided threat assessments to the supervision of these events, as well as members of the State EOC, in preparation for a possible request for assistance.

The CIAC Director was assigned to the EOC during the DNC and provided leadership and situational awareness regarding the DNC intelligence and Emergency Support Function (ESF) 13 - Public Safety and Security coordination. The Director also vetted the information provided by the CIAC to the EOC to ensure that classified information and sensitive investigations were not compromised. The CIAC briefed the EOC personnel on investigations and potential threats during shift changes. EOC personnel thought those briefings were valuable and kept the channels of communication open. The EOC, as well as the other investigative and analytical operations centers, used WebEOC as one of the communication tools to provide FOUO information. Overall, it was noted that additional training and exercises would enhance communication channels and build trusted relationships.[2]

Florida Fusion Center

The FFC is operated by the Florida Department of Law Enforcement (FDLE) Office of Statewide Intelligence, and is a multi-disciplinary all-crimes fusion center. It is designated as the State of Florida's primary fusion center with a focus on terrorism, as directed by State statute. Part of that statute codifies their relationship with the State Division of Emergency Management (DEM) and describes roles and responsibilities for each agency. DEM has responsibility for the State Operations Center (SOC). During steady state, the watch office within the SOC provides 24/7 monitoring of activities and events around the state, and relays any pertinent situational awareness information to the FFC. The FFC also has a 24/7 operational component that serves as the watch, warning and situational awareness element for law enforcement and public safety agencies statewide. The FFC has established an Intelligence Liaison Officer (ILO) program with the agencies that assign personnel to the FFC. These personnel are from State Departments of Health, Corrections, Financial Services, Agriculture, Highway Patrol, Environmental Protection, Education, Attorney General, and Alcohol, Beverage and Tobacco, as well as the Florida National Guard, Federal components of the FFC include DHS, U.S. Attorney's Office, TSA and the Drug Enforcement Agency (DEA). A POC has also been established with the FBI, and two liaison officers from DEM are also assigned to the FFC.

[2] Additional information on the CIAC's role in the DNC is located on LLIS at www.llis.dhs.gov.

The FDLE has identified specific personnel to staff the SOC during activation. This enables the FFC to maintain independent intelligence operations and support to the SOC during incidents. Florida has designated the law enforcement support function as a State of Florida ESF 16 – Law Enforcement and Security. During activation, ESF-16 is led by FDLE with the FFC in a support role. The FFC provides information that is used to address resource needs, assist in planning, and deploy prevention-related resources. Both the FFC and the SOC have necessary facilities to receive and store classified material up to the Secret level. In addition, the FFC has access to Homeland Secure Data Network (HSDN). Security protocols have been developed to address the handling and storage of this information, and the State security officer monitors the handling of this material, and provides oversight on clearance matters for both of these entities.

The FFC and SOC have a Memorandum of Understanding (MOU) in place that describes their respective roles and responsibilities, and each has also established MOUs with their respective participating agencies to memorialize their working relationships. Additionally, the FFC developed a privacy policy that has been shared and adopted by the SOC. The FFC and SOC have also supported the cross-training of personnel, by ensuring select DEM personnel receive basic ILO training from the FFC. These personnel also attend monthly intelligence meetings.

The FFC and SOC have responded to several natural disasters and man-made events, as well as participated in a yearly table top exercise, which has enabled them to test their processes and procedures. Ultimately, protocols and personal relationships have been enhanced by these activities.

SOC and FFC personnel noted that workshops to familiarize all partners enhance mutual understanding of what information is available and how it can be shared. They also noted that this coordination avoids a single point of failure in the event that an incident put one or the other off-line.

Georgia Information Sharing and Analysis Center

In 2007 the Governor of Georgia merged the Georgia Emergency Management Agency (GEMA) and the Office of Homeland Security (OHS), creating GEMA-OHS. This created uniform operating procedures and direction from leadership. The GISAC is operated by the Georgia Bureau of Investigation (GBI), but falls under GEMA-OHS. At the cabinet level, the Director of the GBI and the Director of GEMA-OHS both report directly to the Governor of Georgia.

The GISAC is staffed with personnel from state, local and federal agencies. Currently the GISAC is manned by personnel from the GBI, GEMA-OHS, the Georgia State Patrol, the Georgia Department of Corrections, and representatives from the Georgia Chief's of Police Association, the Georgia Sheriff's Association and the Georgia Fire Chief's Association. Federal partners working in the GISAC include U.S. Immigrations and Customs Enforcement and DHS. The GISAC is also co-located in the same building with the Atlanta FBI-JTTF. Briefings are conducted each morning between GISAC supervisors and members of the FBI JTTF.

The SOC maintains Communications Operations (COMMO) 24/7 during steady-state operations. COMMO handles all after-hours calls for partner agencies and directs calls and reports for the agencies as they are received. COMMO operators have written protocols which are followed regarding the handling of calls and notification procedures. This includes the notification of GISAC on-call personnel after-hours. The SOC sends a morning brief to the GEMA-OHS Director and other senior officials to include GISAC supervisors.

Communications between the GISAC and the SOC are well established and practiced, despite no formal SOPs for sharing information between the two entities. Both entities recognized that this was a direct result of the personal

relationships and communication between each center's leadership. While it was noted that a SOP to codify such interaction may be advantageous, relationships between fusion center and EOC staff benefitted from strong leadership collaboration and communication.

While no specific joint exercises or trainings between the GISAC and SOC are in place, it was noted that these activities may be unnecessary since the two entities coordinate and collaborate on such a regular basis. Additionally, whenever there is a State or regional exercise, all pertinent entities are involved. However, GEMA-OHS and GISAC noted that the future development of common training scenarios, exercises, and SOPs would further enhance existing relationships.

Louisiana State Analytical & Fusion Exchange

LA-SAFE was designated as the State's primary fusion center for gathering, processing, analyzing and disseminating information related to terrorism, homeland security and law enforcement. As such, it is responsible for monitoring threats and providing its partners and stakeholders with situational awareness on a 24/7 basis. LA-SAFE is located on the Department of Public Safety compound in Baton Rouge.

The State EOC is operated by the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) and is located on the same compound but is not co-located with LA-SAFE. Two GOHSEP analysts are assigned to LA-SAFE and serve as liaisons between the two entities. The two entities normally use WebEOC to post and share information, and the GOHSEP analysts are also able to receive information up to the Law Enforcement Sensitive (LES) level. The EOC is activated during select exercises and major incidents that require extensive interagency communication. During those times, LA-SAFE regularly provides the following in support of the State EOC:

- Updated situational assessments;
- Situation reports (SitReps);
- Analytical support;
- Provision of all documents and reference materials, including Geographic Information System (GIS)[3] overlays, graphics and timelines and video teleconference capability; and,
- Additional support as needed.

During Hurricane Gustav, LA-SAFE supported the GOHSEP by using GIS to plan evacuation routes, identify assets that needed protective measures put in place, and indentify resource availability. More recently, they participated in the NLE 2009 exercise, which was focused on prevention and enabled the entities to familiarize themselves with each other's capabilities. Ultimately, the respective roles and responsibilities that guide interaction between LA-SAFE and the State EOC are defined by SOPs, which are currently undergoing revision.

Michigan Intelligence Operations Center

The Michigan State Police (MSP) commands the MIOC, the State EOC and the MSP Watch Office, which is co-located with the MIOC. The MIOC and the State EOC are not co-located and there is no formal agreement on details how the two entities will interact.

[3] See *State & Local Fusion Centers: Developing Processes to Acquire and Use Geospatial Information to Support All Hazards Planning & Response* for more information on uses of GIS.

A MSP Lieutenant is assigned to manage each entity. While the Lieutenants at the fusion center and Watch Office share the same Captain, the Lieutenant at the EOC reports to a different Captain who is responsible for all emergency management functions. All three Lieutenants work closely together and have many overlapping duties, and when the EOC is activated, the MIOC virtually supports the ESF-13 function.

Additionally, each Lieutenant receives and transmits information from sources such as the DHS National Operations Center (NOC), DHS I&A, the FEMA Regions, and other State agencies. These three functional components leverage several tools to ensure thus information is shared with each other, including Homeland Security Information Network (HSIN), and WebEOC, which is also relied upon during partial and full activations. The Watch Office provides situational awareness for events across the state, such as information on road closures and incidents that affect the MSP, while the MIOC prepares a daily open-source briefing and other specialized products for the EOC and its partners. The MIOC and the EOC also conduct between six to nine joint exercises a year in order to test and improve their working relationships. These exercises are supplemented by training on NIMS, which has been provided to both entities.

These processes and training are also well tested during actual events. For example, when the EOC was activated during the NCAA men's final four basketball tournament, the MIOC developed a threat assessment prior the event and provided analytical assistance during the tournament. However, the MIOC and EOC noted that the strong communications between them would be enhanced by the development and implementation of SOPs, as well as through the participation in scenario-driven exercises. These exercises would serve to increase awareness of their respective information requirements, particularly before an event or during a steady state.

Virginia Fusion Center

The Virginia State Police (VSP) and Virginia Department of Emergency Management (VDEM) have a model relationship. The VFC and the Virginia State EOC are co-located and have developed mutually supportive policies and procedures.

Virginia State legislature designated the VFC as the multi-agency fusion intelligence center for Virginia to be operated by VSP in cooperation with VDEM. A MOU further defines the relationship between the police department and the VDEM. The VFC incorporated the policies and procedures for interaction between the VFC and VDEM in its SOPs, which defines the roles and responsibilities of the participants.[4]

A VSP First Sergeant, VDEM Special Assistant for Commonwealth Security and VSP Supervisory Analyst share the management responsibilities for the VFC. The VDEM provides the fusion center with analytical personnel who work side-by-side with VSP and other agencies' analysts; all personnel are cross-trained, are cleared to the same security level, and have the same level of access to sensitive information. The watch offices for both the VFC and the EOC regularly exchange information.

Analysis

Several factors are directly linked to the success of the interaction between fusion centers and EOCs. The first is a spirit of cooperation and collaboration between agencies, which helps build relationships of trust such as the one found in Virginia. Co-location, and the constant contact it offers, may help to facilitate the development of these relationships, but it is not always possible given financial and physical limitations. When co-location is not an

[4] The VFC's MOU and other SOPS are located on LLIS at www.llis.dhs.gov.

option, the EOC and fusion center should arrange regular meetings, training events, workshops, and exercises to build relationships. The resulting familiarity will make for a seamless transition from steady state to activation.

Regardless of whether the EOC and the fusion center share physical space, their interaction should be clearly defined, mutually agreed upon, and formalized by legislation and other documents. These include MOUs and SOPs, which can potentially serve as an annex to the fusion center's CONOPS and/or the EOC's emergency operation plans (EOPs) across the steady state and during activation. The SOPs between the two entities should address how information will be shared, with whom, and under what circumstances (e.g. daily interaction with a watch desk, level of interaction during an incident). They should also describe the process for the exchange and cross-training of agency personnel during both steady state and activation, and the interface with applicable ESFs during activation.

Other relationship-building mechanisms are the Fusion Liaison Officer (FLO) or TLO programs, both of which can expand the fusion center's access to the first responder and emergency management communities. Including EOC personnel in a FLO program will ensure strong connections and familiarity with the fusion center.

Based upon the analysis of the previously identified fusion center and EOC relationships, the following represent potential solutions that should be explored, either separately or in tandem with one other, for enhanced cooperation:

- **Co-location:** Co-location is an ideal way to foster strong relationships between a fusion center and EOC, due to the trust and understanding that develops through continuous contact and interaction. This may not be feasible in many jurisdictions; therefore, virtual communication and collaboration platforms should be explored.

- **Policy and Procedure Documentation:** SOPs and MOUs should be developed to formalize the agreed upon relationships and any associated roles and responsibilities. These will also serve as a basis to train personnel. This documentation should also address access to, handling, and sharing of classified and unclassified information, to include personnel with clearances and access to systems used to transmit information and intelligence.

- **Training:** Any identified liaisons/representatives should undergo extensive cross-training on fusion center and EOC operations to ensure they are intimately familiar with both entities. Fusion center and EOC staff should also have the opportunity to familiarize themselves with the operations of each center, as well as all of the appropriate systems or tools being leveraged. This will assist with building personal relationships between staff from the two entities. Additionally, joint training in security (handling, storage, 28 CFR Part 23, etc.) and classification ([LES, For Official Use Only [FOUO], Protected Critical Infrastructure Information [PCII], classified, etc.) matters, as well as emergency management and incident response frameworks (National Incident Management System [NIMS], National Response Framework [NRF], Incident Command System [ICS], etc) will greatly enhance the understanding of how to appropriately interact and share information.

- **Exercise:** Fusion centers and EOCs should regularly conduct joint scenario-based tabletop and live training exercises to assess their communication capabilities and the exchange of operational information identified in their SOPs and MOUs. These exercises should also serve to evaluate and deconflict the roles and responsibilities of any personnel responsible for the coordination and/or integration of these efforts. The SOPs should be regularly updated based upon the results of the exercises.

- **Communication Systems:** Fusion Centers and EOCs should examine the communication tools available to them and leverage those that provide the greatest connectivity and best enable the entities to share operational information and products, such as alerts and warnings. Discussions between the fusion center and the EOC should address classification levels of the systems, access, training, and limitations on what can and cannot be shared. Additionally, video teleconference (VTC) and secure VTC (SVTC) capabilities should be discussed along with alternate mechanisms for sharing sensitive or classified information (i.e., HSDN).

There are also several personnel approaches that can be used to build and maintain relationships between EOCs and fusion centers, including:

- **Identification of Liaisons/Representatives**: There should be an identified liaison/representative between the fusion center and the EOC whose primary responsibility is to ensure coordination between the two entities. This may be a part-time or ancillary duty. The roles of this liaison/representative should be clearly documented and defined.

    - **ESF-13:** Consideration should be given to using fusion center personnel to staff the ESF-13 function during EOC activation. It will increase the ability of the fusion center to support the EOC with analytical capabilities and will provide reach-back capabilities to Federal, State, and local intelligence resources.

- **Assignment of Full-time Analysts/Personnel:** Based upon available resources, the EOC or responsible emergency management agency should consider assigning or detailing a full-time analyst to the fusion center. This analyst would have intimate knowledge of emergency management operations and serve as a subject matter expert (SME) on emergency management/response operations. The analyst's responsibilities would include providing SME support to fusion center operations and analysis and ensuring the timely and accurate flow of information between the fusion center and EOC before, during, and after incidents.

  Additionally, a fusion center should consider assigning or placing an intelligence officer with appropriate clearances within the EOC during activation. This will ensure the continuous and vital flow of information and intelligence to the EOC, as well as reach-back for support from the fusion center.

- **Unification or Virtual Connection of Watch Offices/Desk:** The watch offices or duty desks of both the fusion center and EOC should consider virtually unifying to ensure that communication is exchanged in the most timely and accurate way possible. This would allow for the timely exchange, coordination, and/or deconfliction of information while serving as a mechanism to formally integrate the fusion center's prevention efforts with the EOC's response efforts. This arrangement would also leverage finite resources/personnel.

- **Expansion of FLO Programs:** Existing FLO programs should be considered as a mechanism to enhance communication between the fusion center and the EOC, especially if dedicated analysts or liaisons responsible for this interaction have not been identified. Emergency management personnel should be considered for inclusion in the program, if they are not yet participating. If a FLO program does not yet exist, the fusion center should consider implementing it in order to build relationships with the EOC via multidisciplinary and SME personnel (e.g. fire, EMS, emergency management, and public health entities).

This page intentionally left blank.

Appendix D: Developing Processes to Acquire and Use Geospatial Information to Support All-Hazards Planning and Response

DHS/DOJ Fusion Process Technical Assistance Program and Services

United States Department of Justice

Fusion Center Spotlight

State & Local Fusion Centers: Developing Processes to Acquire and Use Geospatial Information to Support All Hazards Planning & Response

Background

A number of State & Local Fusion Centers (SLFCs) are at various stages in developing formalized processes and procedures for requesting, accessing, and using geospatial data to support all hazards planning and response efforts. SLFC recognition of the need for and usefulness of this information oftentimes is preceded by a large-scale event, as was the case with the 2005 hurricane season and the summer 2008 Midwest floods. Useful geospatial data can run the gamut from before/after aerial photography or satellite imagery to point locations of water intakes in a flood plain to the locations of critical infrastructure and key resources (CIKR) assets across an entire state. SLFCs should engage in thoughtful planning so that they are prepared to request, access, and use geospatial resources efficiently.

Issues for Consideration

Collection Requirements Coordination

Pre-event coordination between the fusion center, State/regional Emergency Operations Center (EOC), U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) Region, FEMA Headquarters, and the State National Guard is a key element of success. Ideally, this coordination should take place well in advance of a serious man-made or natural hazard event to make sure that a pre-existing process is in place for identifying and tasking potential collection resources. Key local and regional participants in this ongoing partnership include the following or their equivalent:

- Fusion Center Director
- State Geographic Information Systems (GIS) Program Manager
- State EOC Planning Chief
- DHS Office of Intelligence and Analysis (I&A) Intelligence Representative to the fusion center
- State National Guard GIS Planner and/or J2/3 Representative
- FEMA Region GIS Coordinator
- DHS Office of Infrastructure Protection Protective Security Advisors, Regional Geospatial Analysts, and Regional Information Exchange Brokers

This formal or informal Collection Board is in the best position at the State/Regional level to determine what geospatial collection assets can be leveraged against a particular problem set; how to collaborate to prioritize collections efforts; and the best method to task scarce collection resources efficiently.

Baseline Geospatial Data
Prior to submitting any request for new geospatial data, the Collection Board should first have a clear understanding of what baseline data is already on-hand. This includes imagery, point location (e.g. smaller CIKR assets), linear (e.g. rail lines and electric transmission lines), and polygon datasets (e.g. larger CIKR assets such as military bases). Potential data sources that can be surveyed for accuracy and completeness as part of this review include:

- State GIS Clearinghouse
- Classified DHS Tier lists
- Unclassified data contained in Constellation/Automated Critical Asset Management System (C/ACAMS)
- Unclassified data contained in the Homeland Security Infrastructure Program that is accessible via DHS Earth and the DHS Integrated Common Analytical Viewer
- FEMA's Hazards U.S. (HAZUS), software that maps and displays hazard (earthquake, hurricane winds, and flooding) data and the results of damage and economic loss estimates for buildings and infrastructure

Requesting New Geospatial Data
Once the Collection Board has a good understanding of what data is already available, they can better assess what gaps exist that they might want to fill in advance of a large-scale hazard event or in the midst of one. The type of data perhaps most often needed after a natural hazard event has occurred is post-event imagery. This data can be used to better assess damage to areas and the level of damage, lingering flood areas, usability of road and rail corridors, etc. It is important for the Collection Board to understand the various types and classifications of available products and what can be derived from them, , as well as how to request specific information, such as through I&A's State and Local Support Request (SLSR) process or the National Response Coordination Center (NRCC). A good example is from the June 2008 floods in Indiana, in which classified imagery was the only type available in a timely fashion to meet collection requirements. However, most State & local government entities that needed the data did not possess clearances. As a result, the National Geospatial-Intelligence Agency (NGA) was able to produce Unclassified-For Official Use Only (U-FOUO) linear graphics derived from the classified imagery to meet State & local requirements.

One-Stop Shop Dissemination
Just as important as understanding the full range of available information is the ability of the fusion center and other State & local customers to access as much data and related products on a single web-based system or platform. During the 2008 Midwest floods, newly acquired imagery and derived products were made available on a variety of systems, including the Intelink-U Intellipedia, NGA Web-based Access and Retrieval Portal, Homeland Security Information Network-Emergency Management, National Guard systems, as well as Homeland Secure Data Network e-mail. This created access and data availability issues that could be addressed substantially by staging as much U-FOUO data and content as possible on the Intellipedia website, which functioned very effectively and was identified post-event as a best practice. However, if Intelink-U/Intellipedia is to be used to its fullest capability during and after a large-scale hazard event, State & local stakeholders must ensure that all who require account access account have done so as part of the pre-event planning and coordination process.

Recommendations

As SLFCs reach the goals outlined in the *Baseline Capabilities for State and Major Urban Area Fusion Centers,* each will have to address the issues of acquisition, use, and further dissemination of geospatial information and products to a variety of customers. This entails understanding SLFC customer geospatial needs, what data is already available, what gaps exist, how to prioritize and task for collection or construction of datasets, and then how to process and package the information in a format that meets customer needs while ensuring the integrity of the process. As SLFCs begin to identify these requirements and scope the associated issues, they should ensure that all state / regional key partners are represented. The issues for consideration above provide a simple outline for the initial discussions among geospatial stakeholders.

This page intentionally left blank.

Appendix E: Public-Private Partnerships: Safeguard Iowa Partnership's Code of Conduct Manual for Liaisons Serving at Emergency Operations Centers

FEMA Lessons Learned Information Sharing LLIS.gov

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

PRACTICE NOTE

Public-Private Partnerships: Safeguard Iowa Partnership's Code of Conduct Manual for Liaisons Serving at Emergency Operations Centers

PRACTICE

The Safeguard Iowa Partnership (SIP) has developed a code of conduct manual to guide its liaisons serving in emergency operations centers (EOC). The code of conduct manual helps to ensure that all SIP liaisons understand their roles and responsibilities while at an EOC.

DESCRIPTION

SIP is a private sector coalition dedicated to strengthening Iowa's capacity to prevent, prepare for, respond to, and recover from natural and man-made disasters through public-private collaboration. The Iowa state EOC (SEOC) or a county EOC may request that SIP deploy one or more liaisons to its facility during an incident, depending on the magnitude of the incident. SIP liaisons serve as a conduit of information and guidance between the EOC and private sector organizations. During response operations, SIP liaisons facilitate the private sector's donation of supplies, including water, food, ice, and clothing. They assist the EOC's donations management coordinator, but SIP liaisons do not lead the donations operation. SIP liaisons also provide the EOC with information regarding private sector issues, such as operational timelines, facility locations, building access needs, transportation needs, relocation logistics, security issues, and recovery priorities.

SIP partners reduce the impact of emergencies upon their communities by supplementing government preparedness and response capabilities with their own resources and expertise. For more information on SIP, please refer to *Lessons Learned Information Sharing*'s Good Story, The Safeguard Iowa Partnership.

A SIP liaison at the Iowa SEOC coordinated volunteer services and resource donations during the summer storms in 2008. SIP facilitated public-private coordination, which improved the SEOC's overall response efforts. However, at the time of the storms, SIP had not developed guidelines for its liaisons serving in EOCs. After the conclusion of the response operations, SIP decided to develop a code of conduct manual to support and guide its liaisons serving at EOCs during future activations.

For more information on SIP's participation in the 2008 summer storm response, please see SIP's after-action report, *Safeguard Iowa Partnership After-Action Report, September 2008*.

The SIP code of conduct manual addresses liaison qualifications and responsibilities. Before an individual may serve as a SIP liaison, he or she must receive training on EOC operations and be fully knowledgeable about incident management. Each SIP representative must:

- Be familiar with the names and types of various private sector organizations and functions;
- Have strong oral and written communication skills as well as problem assessment and evaluation skills;
- Be proficient with word processing, spreadsheet, and database programs;
- Complete a series of independent study (IS) courses offered by the Federal Emergency Management Agency's Emergency Management Institute:
  - IS 100: Incident Command System,
  - IS 700: National Incident Management System,
  - IS 701: Multi-Agency Coordination System, and
  - IS 775: EOC Management and Operations; and
- Complete training sessions on:
  - Business Resource Registry,
  - Health Alert Network,
  - Homeland Security Information Network, and
  - WebEOC.

WebEOC is a Web-enabled crisis information management software tool that delivers real-time data to emergency managers and responders. The software enables users to share data through message boards, geographic information systems-based maps, resource catalogues, and other tools.

Each SIP liaison must be sponsored by his or her employer in order to serve at an EOC. Additionally, as a volunteer, each liaison must maintain responsibility for all of his or her own travel, lodging, and expenses.

The code of conduct manual also specifies liaisons' responsibilities while at an EOC during an activation. Once a SIP liaison arrives at an EOC, he or she must report directly to the EOC's liaison officer to receive a set of operating procedures, logistical information, and equipment. Typically, EOCs provide liaisons with a computer, Internet access, printing capabilities, a landline telephone, fax machines, and office supplies. The SIP manual suggests, however, that each liaison also bring a personal cellular phone and charger to use as a back-up in case the EOC experiences communication problems. Liaisons must staff a full EOC shift as established by the emergency manager on duty. The SIP manual also requires liaisons to wear business casual attire at all times while serving at an EOC.

LINK

Safeguard Iowa Partnership
http://www.safeguardiowa.org

CITATIONS

Haberl, Jami. Executive Director, Safeguard Iowa Partnership. Interview with *Lessons Learned Information Sharing*, 09 Jul 2009.

Safeguard Iowa Partnership. *Safeguard Iowa Partnership After-Action Report, September 2008*. Sep 2008.
https://www.llis.dhs.gov/docdetails/details.do?contentID=32905

DISCLAIMER