DRAFT DOCUMENT, DO NOT SITE

United States
Department of Justice

DHS/DOJ Fusion Process Technical Assistance Program and Services

Considerations for Fusion Center and Emergency Operations Center Coordination

Comprehensive Preparedness Guide (CPG) 502 - DRAFT

September 2009

FEMA

This page intentionally left blank.

PREFACE

In order for there to be successful interfacing and cooperation between fusion centers and emergency operations centers (EOCs), a familiarity should be built with each other's roles and capabilities. In addition to understanding roles and capabilities, it is imperative that the two develop a solid relationship in order to effectively work together to achieve the objectives of each. 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. Policies on how they will interact should grow out of mutual trust and respect, paving the way for effective operations in steady state and emergency operations. In addition to formalizing a relationship through development of a joint concept of operations, standard operating procedures should be created, reviewed and updated to define the roles of each entity on a daily basis and during periods of activation. Familiarization with and definition of the processes for information flow is only the beginning of the relationship. Both the fusion center and the EOC should make it a part of their concept of operations (CONOPS) and standard operating procedures (SOPs) to ensure continuous contact and exchange of information to improve public safety across the *prevention, protection*, *response and recovery* mission areas. This planning guide 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 private industry, 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) 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 (PMI-SE); 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 added value to the clarity of policies and procedures that guide the sharing of information. Additionally, 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 was released in September, 2008 and 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 (which will be discussed in greater detail later in this guide) call for a policy to 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 included representatives from:

National and Federal Entities:

- CPG Working Group
- DHS Office of Intelligence and Analysis
- FEMA National Preparedness Directorate
- National Fusion center Coordination Group (NFCCG)
- Criminal Intelligence Coordinating Council (CICC)

Industry, Research Organizations, and Universities

- Argonne National Laboratory: Center for Integrated Emergency Preparedness
- CRA, Inc.
- IEM

CONTENTS

1. INTRODUCTION AND OVERVIEW

INTRODUCTION

> ***Fusion Center:*** A *fusion center* is defined as a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

The fusion process is a cornerstone for the effective prevention of terrorism and other crimes by State, Territorial, Tribal, and Local 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 private industry. 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.

The overall goal of the fusion process is to convert raw information and intelligence into actionable knowledge, and fusion centers are effective mechanisms for steering this process. With a network of over 72 fusion centers established across, State Territorial, Local, regional and Tribal governments, are working with the Federal agencies and the intelligence community in accomplishing the National Priorities of *Expanded Regional Collaboration* and *Information Sharing and Collaboration* as defined by DHS's National Preparedness Guidelines.

EOCs 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 events.

Successful implementation of these information requirements requires willing partners (who understand each others' 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 as a cornerstone to support a more coordinated, timely, and effective response to emerging incidents or threats, as well as the integration of traditionally law enforcement-focused *prevention* efforts with traditionally emergency management-focused *response* efforts.

Emergency Operations Center (EOC): 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, law enforcement, medical services), by jurisdiction (e.g., Federal, State, regional, tribal, city, county), or by some combination thereof.

PURPOSE

The purpose of this document is to provide 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 should serve to support implementation efforts of the *Baseline Capabilities for State and Major Urban Area Fusion Centers* and should likewise assist EOCs fill their missions in both steady state and emergency operations as supported by the *CPG 601: Design and Management of Emergency Operations Centers*, which 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 the fusion process:

- Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007
- National Response Framework
- National Criminal Intelligence Sharing Plan
- National Strategy for Information Sharing
- Fusion Center Guidelines
- Baseline Capabilities for State and Major Urban Area Fusion Centers
- Information Sharing Environment (ISE) Implementation Plan
- Information Sharing Environment (ISE) Guideline 2
- National Preparedness Guidelines
- Comprehensive Preparedness Guide (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 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 called for funding for law enforcement/terrorism prevention activities, including: information sharing and analysis, target hardening, threat recognition, and terrorist interdiction.

National Response Framework, Emergency Support Function 5 – ESF -5 coordinates incident 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.

National Response Framework, Emergency Support Function 13 - ESF-13 facilitates coordination of public safety and security among Federal, State, Tribal, and Local 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, Tribal, and Local resources, or when protective solutions or capabilities unique to the Federal Government are required, especially in pre- or

post-incident situations. Activated ESF-13 may provide protection and security resources, planning assistance, technology support, and other technical assistance to support incident operations.

National Criminal Intelligence Sharing Plan - The National Criminal Intelligence Sharing Plan was first published in October 2003 and revised in July 2005. The Plan is designed to link Federal, State, Tribal, and Local law enforcement agencies to develop and 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 Criminal Intelligence Coordinating Council (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 the Department of Justice and with the Justice Intelligence Coordinating Council to improve the flow of intelligence 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 and to improve interagency information sharing at the Federal level and building 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 and tribal 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 - The Department of Justice, in collaboration with Department of Homeland Security and the Federal Bureau of Investigation, developed its first fusion center guideline for law enforcement, intelligence, public safety, and private sector communities, to effectively implement ways to develop

and operate fusion centers throughout the country. The Guideline makes specific recommendations on law enforcement role, governance, IT needs, and information security to better protect our homeland and maximize crime-fighting efforts. The FY 2009 Homeland Security Grant Program also prioritizes the integration of and/or coordination between fusion centers and EOCs.

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 its objectives. Baseline capabilities are labeled under Fusion Process Capabilities; and Management and Administrative Capabilities.

Information Sharing Environment (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 counterterrorist efforts amongst the Federal, State, Local, and Tribal governments and other ISE partners.

Information Sharing Environment (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, and Tribal governments, law enforcement agencies, and the private sector. It requires the construction and implementing the framework for "homeland security information," "terrorism information," and "law enforcement information."

National Preparedness Guidelines - Implemented under the authorization of the HSPD-8, the 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.

Comprehensive Preparedness Guide (CPG) 601: Design and Management of Emergency Operations Centers - CPG 601 is a new Federal guidance document to cover the broad capability requirements of an Emergency Operations Center. It supersedes Emergency Operations Center (EOC) Civil Preparedness Guide 1-20, Emergency Operations Center Handbook (CPG 1-20) that was written in 1984 and was 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. Chapter I addresses the applicability, authority, purpose, and scope of this CPG. Chapter II outlines the roles and initiatives of Federal departments. Chapter III and IV detail how

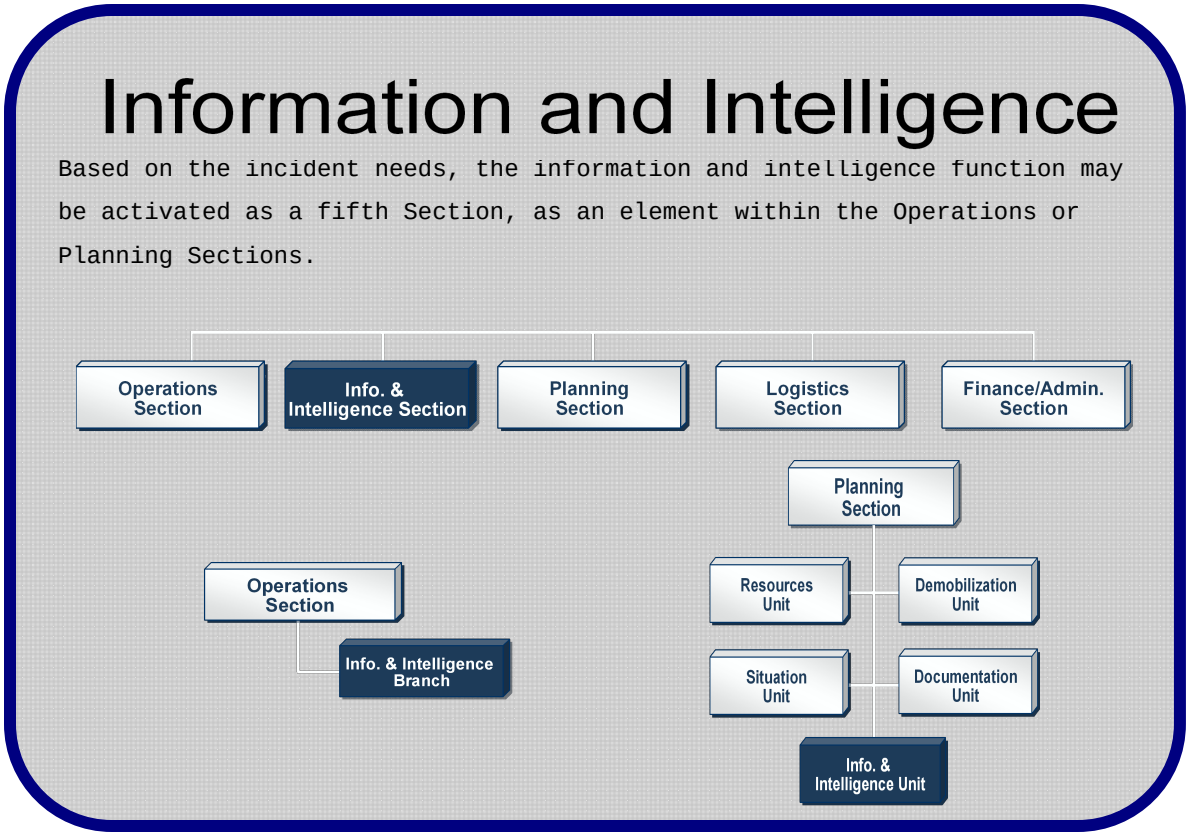
fusion centers and EOCs function, within the broader context of the information sharing environment. Chapter V describes how fusion centers and EOCs may consider coordinating with each other for intelligence and information sharing, and Chapter VI provides case studies about this coordination. The appendices to this guide are as follows:

- Appendix A: Glossary and Acronyms
- Appendix B: Draft Memorandum of Understanding (MOU)
- Appendix C: Federal Intelligence Community Members

NIMS Compliance and Integration

In November 2005, the National Integration Center (NIC) published guides for integrating National Incident Management System (NIMS) concepts into emergency operations plans (EOPs). This guide incorporates the concepts and suggestions found in those documents, including incorporation of the Intelligence and Investigation component of NIMS. EOCs focus on emergency management and response while fusion centers develop and share information and intelligence to prevent and protect against incidents. Although the emergency management system and fusion center network may utilize different methods and tools, both share a public safety mission. Integrating the concepts of NIMS can contribute towards effective collaboration in the joint mission space.

The current edition of NIMS Intelligence/Investigations Function Guidance



Document (NIMS I&I) provides guidance on utilizing and integrating the Intelligence/Investigations Function while adhering to the concepts and principles of the NIMS. 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. The figure below delineates the four places in which information and intelligence function may be found within an incident command structure and allows for the Operations Section to be led by fusion center leadership.

RECOMMENDED TRAINING

See Section 5, the EOC and Fusion Center Coordination: Step Four: Training, Workshops, and Exercises.

REVISION PROCESS

DHS will revise this CPG as needed and issue change pages through the publication and distribution system and on-line through a variety of sources (e.g. DisasterHelp [http:disasterhelp.gov] and DHS Lessons Learned Information Sharing [http://www.llis.dhs.gov])

You can provide recommendations for improving this guide to:
DHS/FEMA National Preparedness Directorate
245 Murray Lane, Building 410
Washington, DC 20528-7000
ATTN: PAB – CPG Initiative
Interim E-mail: Donald.lumpkins@dhs.gov

This page intentionally left blank.

2. FEDERAL DEPARTMENTS INITIATIVES, ROLES AND GUIDELINES

FEDERAL INITIATIVES AND ROLES

NATIONAL FUSION CENTER COORDINATION GROUP (NFCCG)

The NFCCG is co-chaired by the DHS Office of Intelligence and Analysis (I&A), the Federal Bureau of Investigation (FBI) and the Criminal Intelligence Coordinating Council (CICC). The mission of the NFCCG 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 goals of the NFCCG are:

- 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
- Develop a coordinated strategy for the sustainment of fusion centers

DEPARTMENT OF HOMELAND SECURITY

The DHS Secretary identified the Office of Intelligence and Analysis (I&A) as the executive agent within DHS for coordinating the Department's activities with fusion centers. As a member of the intelligence community and homeland security, I&A provides a vital link between the intelligence community and Federal, State, Territorial, Tribal, Local, and private sector entities. It works closely with the 16 Federal intelligence organizations and agencies, as well as State, Territorial, Tribal, Local 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 threats, including border security, radicalization and extremism, particular groups entering the US, protection of critical infrastructure and key resources (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.

The Federal Emergency Management Agency (FEMA) National Preparedness Directorate 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. FEMA also supports the development and operation of emergency operations centers (EOCs) to improve emergency management and preparedness capabilities at the Federal, State, Territorial, Tribal, Local, and private sector level through the provision of support via the EOC Design and Management Technical Assistance service and by ensuring NIMS compliance. The National Integration Center (NIC) was developed as a way to provide strategic direction and a national program for NIMS education and awareness throughout the country.

DEPARTMENT OF JUSTICE (DOJ), BUREAU OF JUSTICE ASSISTANCE (BJA)

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 states, territories, and tribal 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, DOJ's Global Justice Information Sharing Initiative's (Global) Criminal Intelligence Coordinating Council (CICC) is composed of members from law enforcement agencies at all levels of government. Members of the CICC serve as a significant voice and advocate for State, Territorial, Tribal and Local law enforcement and fusion centers, supporting their efforts to develop and share criminal intelligence. Because of the indispensable part that State, Territorial, Tribal and local 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 U.S. safe. The advice of members of

the CICC has also been sought by the Secretary of DHS, members of Congress, and representatives of State government.

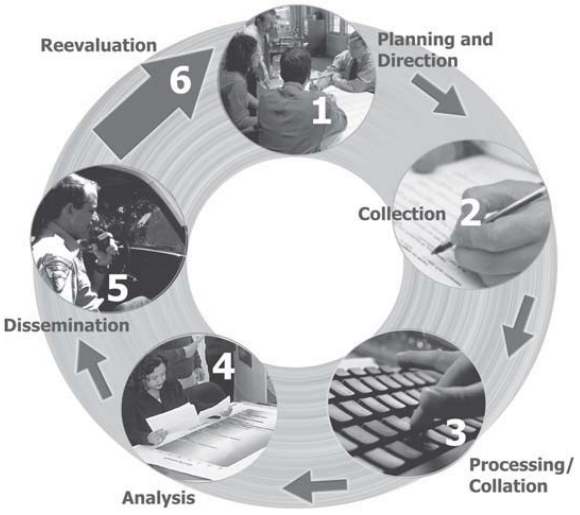
3. THE ROLE OF FUSION CENTERS

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. The process includes the following steps (and is also depicted by the graphic below): 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, 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.

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 private industry. 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, it supports efforts to address immediate or emerging threat-related circumstances and events. Data fusion involves the exchange of information from different sources, including law enforcement, public safety, and the private sector. When combined with appropriate analyses, it can result in meaningful and actionable intelligence and information. 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, Territorial, Tribal, and Local 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.
- Improves the delivery of emergency and non-emergency services.

Actionable Intelligence

Intelligence should:

- "Paint a picture"
- "Tell a story"
- "Guide the response"
- Produce knowledge upon which a course of action can be rested

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 total, 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 Center

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
2. Management and Administrative Capabilities.

The Fusion Process Capabilities focus on the intelligence process within the fusion center while the Management and Administrative Capabilities focus 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 Section V of this guide.

Fusion Process Capabilities

The Fusion Process Capabilities addresses the intelligence process of the fusion center including intelligence collection, analysis, and dissemination. The intelligence cycle 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:

A. Planning and Requirements Development
B. Information Gathering/Collection and Recognition of Indicators and Warnings
C. Processing and Collation of Information
D. Intelligence Analysis and Production
E. Intelligence/Information Dissemination
F. 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:

A. Management/Governance
B. Information Privacy Protections
C. Security
D. Personnel and Training
E. Information Technology/Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure
F. 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. is designed to provide guidance on general trends) as well as tactical (i.e. is intended for a specific event) and is collected on an ongoing basis. The *National Strategy for Information Sharing* (Strategy) 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 that a fusion center's mission should be defined based on jurisdictional needs.

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 this 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 (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 Priority Intelligence Requirements (PIR). The PIRs, in turn, are used to guide the participants in the fusion process and their information collection efforts.

State, Territorial, Tribal, and Local governments, as well as private sector entities, are encouraged to work with both State and Urban Area Security Initiative (UASI) Regions to develop a process 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 have included emergency managers, fire, hazmat, 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 need and viability of the fusion centers by broadening their scope beyond prevention.

4. 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, communications, resource allocation and tracking, and information collection, analysis, and dissemination.

Common Operating Picture: An overview of an incident created by collating and gathering information—such as traffic, weather, actual damage, resource availability—of any type (voice, data, etc.) from agencies/organizations in order to support decision-making

EOC Organization and Structure

The Civil Preparedness Guide 1-20, Emergency Operations Center Handbook (CPG 1-20) was the last Federal guidance written in 1984 to cover the broad capability requirements of an EOC. Even though it was revised in 1989, the field of emergency management has changed significantly since then. CPG 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 24 hours a day, 7 days a week, 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 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 Emergency Support Function (communications, public works, engineering, transportation, resource support, etc.) or, more likely, by some combination thereof.

EOCs may also be staffed by personnel 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 (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 emergency 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. Chief elected and appointed officials may be located at the EOC, as well as personnel supporting core functions. Chief elected officials are executive heads of government and are members of the policy group. They have the principal responsibility for policy decisions. The key function of EOC personnel is to ensure that those who are located at the scene have the resources (e.g., personnel, 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 operations centers (referred to as Department Operations Centers, or DOCs) that serve as the interface between the ongoing operations of that organization and the emergency operations it is supporting. The DOC

An EOC is activated:
- To support the on-scene response during an escalating incident by relieving the burden of external coordination and securing additional resources.

An EOC is:
- A physical location.
- Staffed with personnel trained for and authorized to represent their agency/discipline.
- Equipped with mechanisms for communicating with the incident site and obtaining resources and potential resources.
- Managed through protocols.
- Applicable at different 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.
- To provide coordination, direction, and support during emergencies.

An EOC may:
- Facilitate MACS functions and may be needed to support Area Command, IC, or UC when resource needs exceed local capabilities.
- Provide for the transition into recovery.
- Be activated in anticipation of an event.

An EOC does not:
- Command the on-scene tactical level of the incident.

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 agent(s) for the department or agency.

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

EOCs should be both flexible and scalable to be efficient and effective, and 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:

- Situation Assessment
- Incident Priority Determination
- Critical Resource Acquisition and Allocation
- Policy Direction for Relevant Incident Management and Interagency Activities
- Coordination With Other MACS Elements
- Coordination With Elected and Appointed Officials
- Coordination of Summary Information
- Public Information

OPERATIONAL EXCHANGE OF INFORMATION

A primary focus of EOCs is on response and recovery efforts associated with natural and man-made events. While the purpose 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. 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. Any information about 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 on-going events and serve as a warning point during activation.

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 Memorandum of Understanding 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. In jurisdictions where a fusion liaison program is formalized, a cadre of qualified personnel may already exist.

EOC staff should plan to have a capability to access and share information from the fusion center, as well as other sources, and should leverage systems such as the Regional Information Sharing Systems (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 State and Local Fusion Centers are 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 sources, including weather, geospatial and remote sensing imagery, damage assessments, media reports, financial impact, social effects and many others. They may leverage assistance (from fusion center staff for example) in gathering this event-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.

5. THE EOC AND FUSION CENTER COORDINATION

Fully coordinating and/or integrating EOCs and fusion centers 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 in order to develop a long term working relationships, including training and exercising, which complement (not competes with) one another. Open dialogue from the outset will allow both sides to address concerns and develop a governance mechanism to maintain the process.

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 and reports they produce, and their informational needs/requirements. Of particular importance for the EOC, is to be specific on the type of information or intelligence they need, why they need it and on what timetable. This may vary between normal operating times (steady state) and as an event builds up, occurs, (active state) and eventually returns to steady state. If there are particular timetables established for EOC products, such as briefing, or situation reports, ensure the fusion center is aware of them so the fusion center can provide the product or information necessary for EOC usage. 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-hazard” or naturally occurring incidents.

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

A candid dialog of each center’s needs will provide a greater understanding of the others constraints on meeting one another’s needs. Without this dialog, it will be easy to pass a lot of 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.

The following capabilities list is meant to be a starting point and is not intended to be all-encompassing:

Standard Policies and Procedures

Understanding each other's concept of operations (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 track 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. The value of SOPs is particularly important to new personnel assigned to either entity during a crisis or disaster. During future planning sessions, SOPs should be reviewed to ensure they are current. These SOPs should also be trained, exercised and evaluated to ensure they are accurate and applicable.

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.

Communication Tools

- What tools are available for EOCs and fusion centers to send, receive, and manage information?
- 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?

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 are being used or do fusion centers and EOCs 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)
- GIS Capabilities
- Law Enforcement On Line (LEO)
- National Crime Information Center (NCIC)
- Region Information Sharing Systems
- Guardian, E-Guardian
- Homeland Security Information Network
- Homeland Security Data Network
- IT systems and 28 CFR Part 23 issues
- Virtual EOC or other emergency management software applications
- Situational awareness or watch systems
- Other classified and unclassified systems

Staffing

Fusion centers staff law enforcement officials, as well as intelligence analysts and CIKR analysts. Additionally, similar to EOCs, fusion centers also often staff 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. (See Step Two)

When staffing, 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. Those needing security clearances should be indentified, and the fusion center may be able to assist in submitting requests for clearances through DHS.

Training Resources

- What training tools/programs are currently being used by the EOC and fusion center?
- What methods can be used 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 EM staff should be trained on fusion center and intelligence and information sharing protocols, such as:
    - Receiving/handling classified information;
    - Receiving/handling criminal intelligence information in accordance with 28 CFR Part 23,
    - The protection of information privacy and other legal rights in the context of the information sharing environment,[1] and
    - Receiving/handling Protected Critical Infrastructure Information (PCII), Sensitive Security Information (SSI), Chemical-terrorism Vulnerability Information (CVI), and/or Safeguards Information (SGI).
  - Statewide exercise calendar
- What training needs to be developed to fill in any "gaps?"
- Are exercises conducted within the centers as with other entities to build relationships and interoperability? (See Step Four)

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

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 must 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 a fusion center shape the products it produces, or identify gaps in information for which the fusion center or EOC could fill with the creation of new products or reports.

Additionally, EOC's, prior to receiving law enforcement or intelligence information, must develop and maintain a safeguarding policy to ensure this information is handled properly, not shared with media or public, and destroyed properly. EOCs may address this by developing their own policy/plan, adopting the Fusion Centers security policy/plan or via an MOU with the fusion center.

Fusion Center Baseline Capabilities:

I. Fusion Process Capabilities:

D. Intelligence Analysis and Production

10. 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 report, special bulletins which describe threats or crime problems, crime trend reports, officer safety bulletins, Be on the look out for notices (BOLOs), tactical analytical reports, and responses to requests for information (RFI). Unclassified reports 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. This consists of how jurisdiction, 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 on-going 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 Title 28 Code of Federal Regulations (CFR) Part 23 restrictions. 28 CFR Part 23 is a guideline for law enforcement agencies. It 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.

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 the repository for CIKR information that can shared with the EOC during an incident and assist with the 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 well equipped for back up 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 if they have not been established, including identification or sharing of alternative sites and communications capabilities to continue the essential functions of the fusion centers. This coordination between the fusion center and EOC can also support the entities jointly leverage COOP or back-up 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, and 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 a potential act of terrorism). 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.

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

The EOC and fusion center should brief each other on policies, procedures, and protocols. Meetings between EOC and fusion center leaders should be continued 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 each other are familiar with these 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.

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, Memorandums of Understanding (MOUs) need to be formalized. 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.
In addition to this benefit, MOUs may also be used to resolve policy conflicts between parties. However, 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 a 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 a 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 recipient(s) 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).

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)an, if needed, nondisclosure agreements (NDA) between the center and each stakeholder who intends to participate in or partner with the fusion center.

Information exchange procedures between the EOC and fusion center should also take into account existing procedures for the exchange of information between the EOC and 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?

The EOC should use the fusion center as its conduit to communicate information with the intelligence community, as fusion centers can provide direct representation in the EOC (sometimes via a fusion center liaison or through ESF 13) or through a Fusion Liaison Officer or Terrorism Liaison Officer program. Intelligence information should flow through the fusion center and then be sent to the EOC. Conversely, information and intelligence products such as situation reports (SITREPS), incident action plans (IAPs) 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.

The Fusion Liaison Officer 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 and is working to facilitate communication between law enforcement and emergency

management information needs. Fusion Liaison Officers coordinate information sharing activities among the private sector, critical infrastructure and industry 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 regional 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 be aware of, protect against, mitigate, 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.

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 is not compromised. The utilization of these types of 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, 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 National Incident Management System (NIMS) and Incident Command System (ICS).

STEADY STATE VS. ACTIVE STATE

EOC coordinators (as well as law enforcement and other homeland security officials) should be familiar with the operations of the fusion centers. A decision to activate (or partially activate) the EOC based on intelligence from the fusion center may be inserted into EOC plans or protocols.

Different information requirements are associated with a fusion center in "steady state" versus "active state." On a daily basis, fusion centers should be prepared to provide information on potential events to the EOC coordinators. Unfortunately, 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). 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 event.

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

During EOC activations, fusion centers 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 usually, the information can 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 what 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"
> - Produce knowledge upon which a course of action can be rested

STAFFING

The fusion process seeks to eliminate duplicative efforts of fusion center and EOC staff and emergency management planners by taking some of the information collection duties away from the EOC planning section. While the

EOC and the fusion center leverage information that has been gathered, it is the primary and function of the fusion center to analyze the information and disseminate intelligence.

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

- Fusion center management
- State, Territorial, Tribal and/or Local 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 Liaison Officers - ATF, DEA, FBI, DHS (CBP, ICE, USCG, FEMA), etc.
- State or local terrorism liaison coordinators
- Fire service
- EMS
- Public health
- HazMat

The following outlines several potential mechanisms and positions that may serve to directly support the integration and/or coordination of fusion center and EOC operations and exchange of information, and may not be applicable in every jurisdiction.

- **Identification of Liaisons/Representatives:** There may be an identified liaison/representative between the fusion center and the EOC who has a primary responsibility for ensuring coordination between the two entities. This may be a part-time or ancillary duty. The roles of this liaison/representative related to managing the interaction and the exchange of information should be clearly documented and defined.
- **Assignment of Full-time Analysts/Personnel:** The EOC or responsible EMA should consider assigning or detailing a full-time analyst to the fusion center. This analyst would have intimate knowledge of EM operations and serve as an emergency management/response operations SME. Responsibilities of this analyst would include providing SME support to fusion center operations and analysis, and also serve to ensure the timely and accurate flow of information between the fusion center and EOC before, during, and after incidents.

- **Unification of Watch Offices/Desk:** The fusion center watch office and EOC watch or duty office may consider the collocation of watch offices/desks to ensure the most effective means for the timely and accurate exchange, coordination, de-confliction, and communication of information. This would also serve as a mechanism to formally integrate prevention efforts of a fusion center with the response efforts of an EOC, while leveraging finite resources/personnel.
- **Expansion of FLO Programs:** Existing FLO programs may be considered to serve as a mechanism to enhance communication between the fusion center and EOC, especially if dedicated analysts or liaisons/representatives responsible for this interaction have not yet been identified. Additionally, if existing FLO programs do not currently have emergency management personnel participating, the fusion center should consider including this discipline. Lastly, if a FLO program does not exist in a jurisdiction, the fusion center may want to consider implementing this program as a means to build relationships with the EOC via multi-discipline and SME personnel, including fire, EMS, public health, and emergency management, until longer-term and more formalized solutions may be implemented.

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 EXERCICES

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 primer 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 offered by DHS that are applicable for EOC/EM and fusion center personnel are as follows:

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 Framework "establishes a comprehensive, national, all-hazards approach to domestic incident response." http://training.fema.gov/EMIWeb/IS/IS800b.asp.

National Incident Management System (NIMS): IS-700. This course introduces NIMS by explaining its purpose, principles, key components, and benefits. http://training.fema.gov/emiweb/is/is700.asp.

Incident Command System (ICS) 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

FEMA Independent Study—860a National Infrastructure Protection Plan (NIPP). This course introduces the NIPP, identifies relevant authorities for critical infrastructure and key resources (CIKR) protection efforts, and related information-sharing processes. http://training.fema.gov/EMIWeb/IS/IS860a.asp

FEMA Independent Study—821 Critical Infrastructure and Key Resources Support Annex. This course provides an introduction to the Critical Infrastructure and Key Resources (CIKR) Support Annex to the National Response Framework (NRF). http://training.fema.gov/EMIWeb/IS/IS821.asp.

Introduction to Incident Command System (ICS): IS-100.a. This course introduces the ICS and provides the foundation for higher level ICS training. This course describes the history, features and principles, and organizational structure of the Incident Command System. It also explains the relationship between ICS and the 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 the Incident Command System. 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

FEMA Independent Study—813 Public Safety and Security Annex. This course introduces Emergency Support Function (ESF) #13 –Public Safety and Security Annex. http://training.fema.gov/EMIWeb/IS/IS813.asp.

FEMA Independent Study— 775 EOC Management and Operations. This course describes the role, design, and functions of EOCs and their relationships as components of a multi-agency coordination system. The course contains disaster-related examples, activities and case studies that relate to EOC's and multi-agency coordination systems 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/.

E947 - IEMC: EOC-Incident Management Team Interface. 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/training/programs/state-local/training-opportunities/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/training/programs/state-local/training-opportunities/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 www.it.ojp.gov/PrivacyLiberty and www.ise.gov/pages/privacy-overview.html.

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.

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 and it has since 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 (www.NCIRC.gov) Web site, accessible through HSIN Intel, LEO, and RISS. http://www.iir.com/28cfr/Overview.htm.

Chemical-terrorism Vulnerability Information (CVI) Authorized User Training at https://csat.dhs.gov/pls/apex/,DanaInfo=.aadewvjw8Hl2l5M2632Rz8E+f?p=128:1:2339275447493351

Protected Critical Infrastructure Information (PCII) Program Authorized User Training at https://submitcii.dhs.gov/pcii/PCIIAuthorizedUserTraining/

Fusion Liaison Officer (FLO) Programs. FLO Programs, as mentioned earlier, facilitate the development and coordination of a network of fusion center liaison officers who are members of local or regional law enforcement, fire service,

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 Lesson Learned Information Sharing (LLIS) System at www.llis.dhs.gov and the National Criminal Intelligence Resource Center (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.

Fusion Process Technical Assistance Program also facilitates Fusion Center Direct Interaction Workshops, which allows subject matter experts to provide for efficient and effective share of best practices and lessons learned.

EXERCISES

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 the exchange of operational in formation identified in their SOPs and MOUs. These exercises should also be aimed at evaluating and de-conflicting the roles and responsibilities of any identified personnel responsible for the coordination and/or integration of these efforts. 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.

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.

6. CASE STUDIES

Fusion centers play a critical role in providing planning and operations intelligence supporting for special events of various sizes. As the central repository of strategic and tactical information with a region, 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 a National Special Security Event (NSSE), 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, State, Territorial, Tribal, Local 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, Territorial, Tribal, Local and Federal participants, can begin the process of collecting, analyzing and disseminating information and intelligence. The U.S. Secret Service 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 their protectees.

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 who 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 collocated, successful relationships are built on a series of steps that define the roles and responsibilities of the participants. The necessary components are enabling legislation, Memorandum of Understanding 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 Fusion Liaison Officer 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.

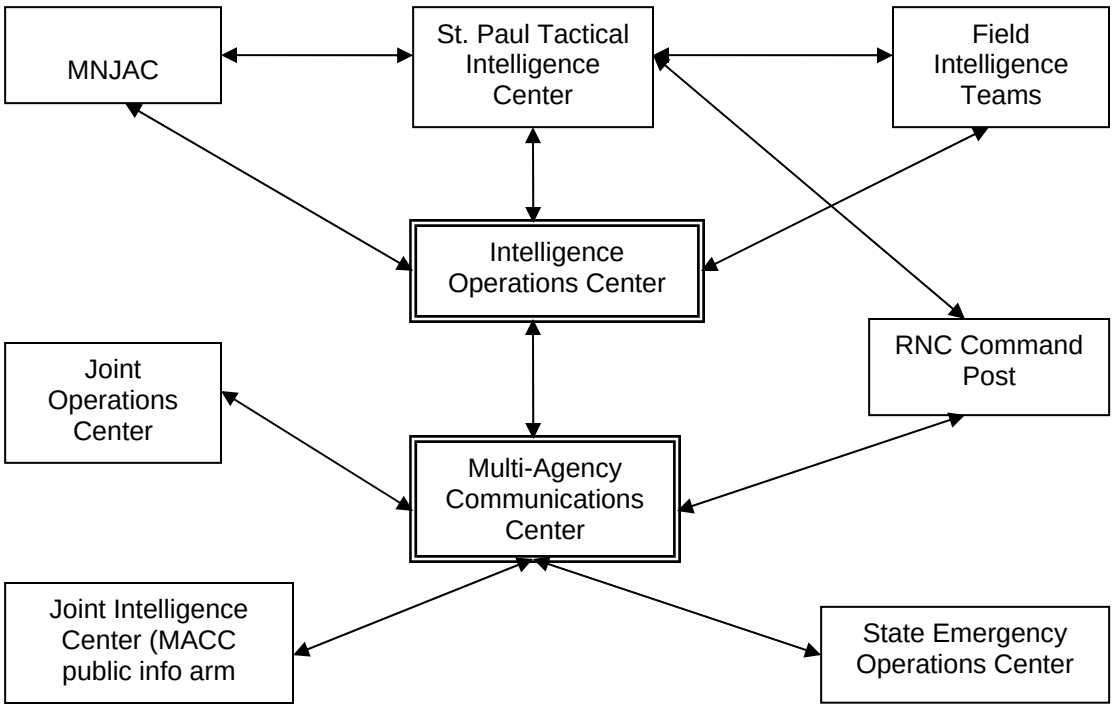
Minnesota Joint Analytical Center and the Republican National Convention

The Minnesota Joint Analytical Center (MNJACP), which is the State fusion center, provided critical information and intelligence support during the Republican National Convention (RNC) held in Minneapolis-Saint Paul, MN on September 1-4, 2008. Because of the NSSE classification, the U.S. Secret Service 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 the Federal Emergency Management Agency, U.S. Coast Guard, Customs and Boarder Protection, Transportation Security Administration, DHS Office of Intelligence and Analysis, Domestic Nuclear Detection Office, U.S. Immigration and Customs Enforcement, Saint Paul Public Works, and the RNC Host Committe.

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 public safety threat and a crowd control issue (law enforcement arrested 818 individuals). During the RNC, the MNJAC had personnel assigned to the TIC and the IOC, which created an efficient flow of information to and from the centers.

MNJAC was able to utilize the Intelligence Communications Enterprise for Information Sharing and Exchange (ICEFISHX) network (which is used to collect information 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 shows how information was shared between numerous stakeholders:



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

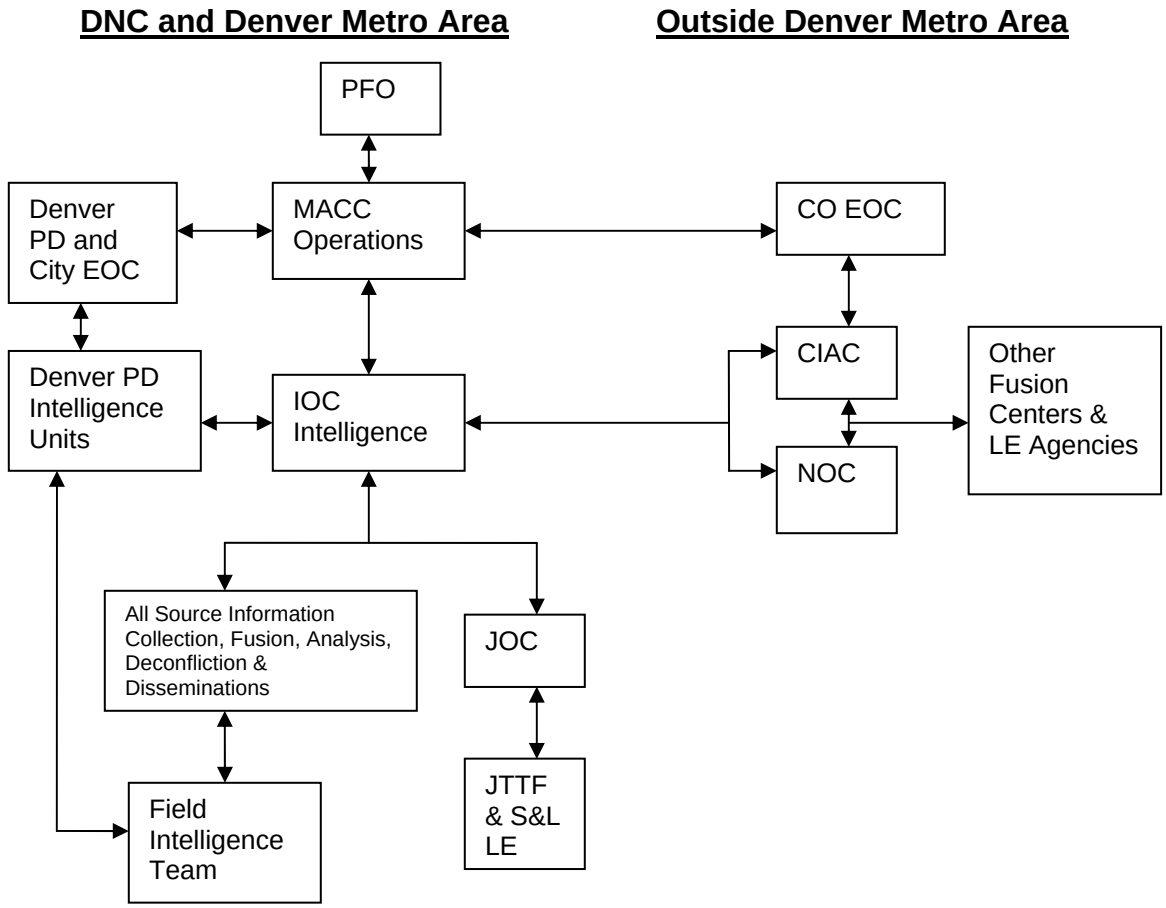
Throughout the RNC and for all accompanying activities, the collaboration and co-location of Federal, State, and local agencies with the private sector provided a supportive environment which resulted in timely exhchange of information and successful management of multiple activities. Specifically, the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

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, CO on August 25-28, 2008. The CIAC is a State fusion center located in a Denver suburb and managed by the Colorado State Patrol and colocated in the same building with the State EOC. The CIAC and the FBI shared equal management responsibility for the Intelligence Operations Center (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 stand-by mode during the event. The CIAC commander was assigned to the EOC and provided EOC leadership and 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 operation within the Denver metropolitan area was coordinated by the IOC. The CIAC, along with the DHS National Operations Center (NOC) in Washington, DC, 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 shows the information flow between the various stakeholders:



Source: DHS/DOJ Fusion Process Technical Assistance Program and Services. Fusion Center Spotlight, 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 multi-agency 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 acitivities. The cooperation between the CIAC and the FBI in running the IOC provides a model for future NSSEs and other special events.

Fore 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 Emergency Operations Center (EOC) Integration and Coordination Workshop: Reference Documents* kit for more information on the operations and interaction of the Colorado Intelligence Analysis Center (CIAC) during the DNC. This document is also located on the Lessons Learned Information Sharing (LLIS) System at www.llis.dhs.gov and the National Criminal Intelligence Resource Center (NCIRC) at www.ncirc.gov.

Analysis of Coordination and/or Integration Best Practices

DHS also conducted site visits to examine the relationship between fusion centers and EOCs, and how they support each other. The purpose of these visits was to determine the capabilities and tools each entity leverages, to identify ways those capabilities could be better incorporated or coordinated, and to identify resources, training and technical assistance to support the coordination and integration efforts. Participating personnel from both entities was interviewed about systems or protocols for communication, formal agreements on interaction, cross-training and exercises to build relationships, types of information being shared, benefits of co-location to information sharing, and ways to enhance the relationship. The following are summaries of such site visits.

Arizona Counter Terrorism Information Center

The Arizona Counter Terrorism Information Center (ACTIC) is one of the most mature and capable fusion centers in the U.S. Their TLO program addresses all-hazards environment and is now embedded in all of the prevention, response, and recovery actvities in Arizona. ACTIC is co-located with a State, county, or local EOC.

ACTIC's TLO program supports EOCs during activations. ACTIC is developing standard operating procedures (SOPs) for TLO participation or liaison with EOCs during an incident, which will be maintained at the ACTIC. According to the interviewed emergency managers, the presence of a TLO in their EOC allowed them access to all of ACTIC's data, which enhanced their ability to respond to any situation. They believed that this mitigated the need to be co-located with the ACTIC. During EOC activation, ACTIC makes all of its non-classified information (not classified above the Secret level) available to the EOC. TLOs are required to sign a non-disclosure agreement in order to protect civil liberties and privacy.

ACTIC frequently conducts exercises and training with State and local EOCs. Its outreach and training programs, the robust analytical and investigative capabilities have enhanced the relationship between the fusion center and its public and private sector partners.

COLORADO INFORMATION ANALYSIS CENTER

The CIAC and the State EOC are located in the same building. The EOC has a watch officer on a 24/7 basis who serves as the link between the EOC and the CIAC. The EOC watch office is on the distribution list for CIAC products, including their daily and weekly reports, as well as any special bulletins. Additionally, the CIAC periodically receives reports and briefings from the EOC watch office. Training between the two entities had not been regularly conducted prior to the DNC. However, the CIAC included EOC and emergency management personnel in the TLO program to ensure understood roles and responsibilities. Some of those personnel were assigned to the various command and control centers activated during the DNC, while others were used to backfill slots in the CIAC.

VIRGINIA FUSION CENTER

The Virginia Fusion Center (VFC) and the Virginia State EOC demonstrate a model relationship. They are co-located and have developed policies and procedures that support each other's operations. A memorandum of understanding also defines the relationship between the two centers. Management responsibilities between the two entities are shared by the Virginia State Police (VSP) First Sergeant and a Virginia Department of Emergency Management (VDEM) Special Assistant for Commonwealth Security. The VDEM provides analytical personnel to VFC, and all personnel are cross-trained and cleared to the same security level. The watch office for both the VFC and the EOC regularly exchange information. The VFC incorporated the policies and procedures for interaction between the VFC and VDEM in its Concept of Operations (CONOPs) and SOPs. The spirit of cooperation between the VSP and VDEM builds trust and overcomes previous misconceptions.

POTENTIAL SOLUTIONS FOR BUILDING FUSION CENTER AND EOC RELATIONSHIPS

Based on the analyses of the previously identified fusion center and EOC relationships, here are some solutions for better cooperation.

Co-location

Co-location is an ideal way to foster strong relationships between the two entities based upon trust and understanding through continuous contact and interaction. However, it is not feasible in many jurisdictions.

Policy and Procedure Documentation
SOPs and MOUs should 1) formalize the agreed upon relationships, associated roles and responsibilties, 2) serve as a basis for training and exercising personnel on these relationships, and 3) address access to and sharing of classified and unclassified information, including those holding clearances and systems used to transmit information intelligence.

Training
Liaisions and representatives should undergo extensive cross-training on fusion center and EOC operations. In addition, staff of each entity should have the opportunity to cross-train to familiarize themselves with the operations of both centers. This will also help build personal relationships.

Exercise
Joint scenario-based tabletop and live training exercises should be conducted to assess communication capabilities and exchange of operational information identified in MOUs and SOPs.

Personnel Approaches

- There should be an identified liaison/representative between the fusion center and the EOC with a primary responsibility of ensuring coordination between the two entities.
- The EOC or emergency management agency (EMA) should consider assigning a full-time analyst to the fusion center who would serve as a subject matter expert (SME) on emergency management operations and response. This person would ensure the timely and accurate information flow between the two centers before, during, and after incidents.
- The fusion center and the EOC watch office should consider the unification or virtual connection of these two offices to ensure the most effective means for the timely and accurate exchange, coordination, de-confliction, and communication of information.
- FLO programs should be implemented or existing FLO programs should be considered as a mechanism to enhance communication between the fusion center and EOC. The fusion center should consider including emergency management personnel in the FLO program if that discipline is not yet represented.

APPENDIX A: GLOSSARY AND ACRONYMS

GLOSSARY

Access (to sensitive information)

Sensitive information and/or intelligence may be released by a law enforcement agency when at least one of the following four prescribed circumstances applies to the person(s) receiving the information.

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 (for example, 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 what 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 and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies (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 Priority Information Requirements.

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

It is 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.

Confidential Classification

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

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 incapacity 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 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, 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—sees CUI Framework for more. (Presidential Memorandum to Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information (CUI), May 7, 2008).

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 private industry. 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)

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 Classification

See Classified Information/Intelligence.

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 of America. 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, and tribal 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 (IC)

The IC 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 Intelligence Cycle or 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.

National Incident Management System (NIMS)

System that provides a proactive approach guiding government agencies at all levels, the private sector, and nongovernmental organizations to work seamlessly to prepare for, prevent, 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 the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) that supports national-level interoperable information sharing.

National Integration Center (NIC)

A multidisciplinary entity made up of federal stakeholders and over time, will include representatives of state, local and tribal incident management and responder organizations. It is situated within the Department of Homeland Security's Federal Emergency Management Agency.

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 a multidisciplinary entity made up of federal stakeholders and over time, will include representatives of state, local and tribal incident management and responder organizations. It is situated within the Department of Homeland Security's Federal Emergency Management Agency.

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)

The Office of Intelligence and Analysis (I&A) is a component of the Department of Homeland Security 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 the Department, at state, local, and tribal 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.

Rule

A specific requirement or prohibition that is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

Secret Classification

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

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)

Sensitive But Unclassified (SBU) Information

Refers collectively to the various designations used, prior to the issuance of the Controlled Unclassified Information framework, within the federal government for documents and information that are sufficiently sensitive to warrant some level of protection from disclosure but that do not warrant classification. (Presidential Memorandum to Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information [CUI], May 7, 2008)

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.

Top Secret Classification

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

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
BJA	Bureau of Justice Assistance
CICC	Criminal Intelligence Coordinating Council
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CPG	Comprehensive Preparedness Guide
CIKR	Critical Infrastructure/Key Resources
DHS	Department of Homeland Security
DOC	Department Operations Centers
DOJ	Department of Justice
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ESF	Emergency Support Functions
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
FLO	Fusion Liaison Officer
GIWG	Global Intelligence Working Group
HSIN	Homeland Security Information Network
IAP	Incident Action Plans
I&A	Office of Intelligence and Analysis
ICS	Incident Command System
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement On Line
LLIS	Lessons Learned Information Sharing
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCIRC	National Criminal Intelligence Resource Center
NCISP	National Criminal Intelligence Sharing Plan
NDA	Non-Disclosure Agreement
NIEM	National Information Exchange Model
NIC	National Incident Management System Integration Center
NIMS	National Incident Management System
NOC	National Operations Center
NPD	National Preparedness Directorate

NRF	National Response Framework
ODNI	Office of the Director of National Intelligence
PM-ISE	Program Manager for the Information Sharing Environment
RFI	Request for information
RISS	Regional Information Sharing Systems
SITREPS	Situation Reports
SME	Subject Matter Expert
SOP	Standard Operating Procedures
UASI	Urban Area Security Initiative
USSS	United States Secret Service
WMD	Weapons of Mass Destruction

APPENDIX B: DRAFT MEMORANDUM OF UNDERSTANDING

This Draft Memorandum of Understanding is provided only as a guide to describe how the fusion center and the EOC will interface. It is not intended as a Memorandum of Understanding to establish a fusion center, or an EOC. Guidance on a Memorandum of Understanding 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 below. 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 a Memorandum of Understanding 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, to indicate 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 MOU is to establish the policies, which 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 that information which 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:

The (Head of State LE 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 LE 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 Emergency Operations Center.

(Insert the composition of the Advisory Board. Consider the board composition to include (Head of State LE or Homeland Security Agency) as the Chair, the State Coordinator of Emergency Management (Co-Chair), as well as representatives from the Governor's Office or Agency/Office of Homeland Security or Preparedness, a representative(s) from legislative branch, representative from the Federal Bureau of Investigations, a representative from the State National Guard, a representative from the Chief's associations representing police, fire, sheriffs, 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 Advisory Board will make recommendations to the Chair regarding the development of policy, resolution of conflicts and ensuring compliance with the Memorandum(s) of Understanding. 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 on-site 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 SOPs 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 Counter-Terrorism Unit (CTU) and the Homeland Security Information and Intelligence Unit (HSIU). 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 agency(ies)/entity(ies) 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, as described above, 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 ESF 14 (Law Enforcement) and may augment other ESF's or EOC operations as requested (i.e. transportation, energy, public health). Depending on the circumstances, this augmentation may be a build-up 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 Command, Operations, Planning, Logistics, and Finance/Admin 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 communications 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 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 utilize state agency personnel from many disciplines, outside resources, and private industry. A Memorandum of Understanding 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 Memorandum of Understanding 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 (i.e. State Police Division Commander) who, through channels reports to the (Head of State LE 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.

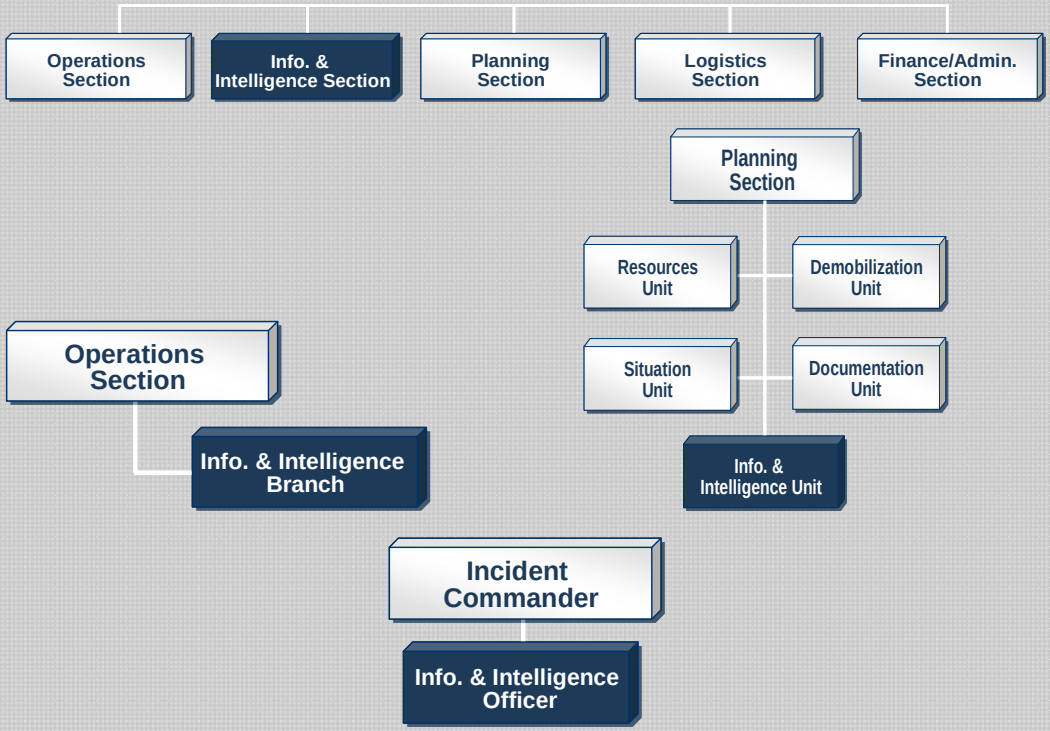
During activation of the EOC, fusion center resources used to augment the EOC will continue to operate within their chain of command when located with in the fusion center. If EOC augmentation requires fusion center personnel to be relocated to the EOC, they shall report to and operate under the EOC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

Problems and difficulties, which 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. Following NIMS:

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 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, verify which EOC organizational element the fusion center resources will be supporting. The following is 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
Intel/Info Section	1 Supervisor 1 Analyst	1 Section Chief 1 Supervisor 3 Analysts 1 Administrative
Ops Section – Intel/Info Branch	1 Supervisor 1 Analyst	1 Branch Director 3 Analysts
Planning Section – Intel/Info Unit	1 Supervisor 1 Analyst	1 Team Leader 3 Analysts
ESF - 14 Support	1 Supervisor	1 Analyst

E. Security Clearances and Classifications of Documents

(*This section defines who has/can be granted security clearances based upon 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 FBI and/or the participating agency. All signatories agree to abide by originator controlled documents and third party dissemination regulations

EOC staff include the State Coordinator, Deputy State Coordinator(s), Operations Section Chief(s) are required to have a secret (or higher) security clearance, Planning Section Chief(s), 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 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 US 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, 28 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 Emergency Operations Center 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, VTCs, temporary storage of classified information up to the secret level. Fusion Center augmented resources on site 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. 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 then 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, with address and consider adding lat/long coordinates as well). The EOC is located at (insert location, with address and consider adding lat/long 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

(This section was designed to 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 LE 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 will provide 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 center's personnel, regardless of the sponsoring agency, will be managed and guided by the Standard Operating Procedures to include 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 LE 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 LE or Homeland Security Agency) investigation, or that of a sponsoring federal agency. Removal from the center(s) and/or elimination of access will be in accordance with the Standard Operating Procedures 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 LE 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 collocated.)*

The fusion center facility will be managed by (State LE 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 (i.e. HSIN, Secure Video and CWIN connections), such as voice and facsimile circuits will remain the responsibility of the State Emergency Management Agency for maintenance and costs. Likewise, similar State LE or Homeland Security Agency circuits, etc. will remain the responsibility of the State LE 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 center(s) 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 out of the acts of the center(s) 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 out of, 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, ay 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 re done 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 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.

1 This page intentionally left blank.