Global Justice Information Sharing Initiative

United States Department of Justice

Baseline Capabilities for State and Major Urban Area Fusion Centers

A Supplement to the *Fusion Center Guidelines*

September 2008

Baseline Capabilities for

State and Major Urban Area Fusion Centers

A Supplement to the
Fusion Center Guidelines

September 2008

About Global

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

This project was supported by Grant No. 2007-NC-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Table of Contents

Introduction 1
- Purpose 1
- Introduction and Background 2

Methodology and Document Structure 5
- Methodology 5
- Document Structure and Use 9

Section I: Fusion Center Capability Areas: Fusion Process Capabilities 11
- A. Planning and Requirements Development 12
- B. Information Gathering/Collection and Recognition of Indicators and Warnings 16
- C. Processing and Collation of Information 17
- D. Intelligence Analysis and Production 18
- E. Intelligence/Information Dissemination 20
- F. Reevaluation 21

Section II: Fusion Center Capability Areas: Management and Administrative Capabilities 23
- A. Management/Governance 23
- B. Information Privacy Protections 27
- C. Security 30
- D. Personnel and Training 31
- E. Information Technology/Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure 33
- F. Funding 34

Appendix A: Focus Group Participants 35

Appendix B: Baseline Capabilities Crosswalk 37

Appendix C: Glossary of Terms 43

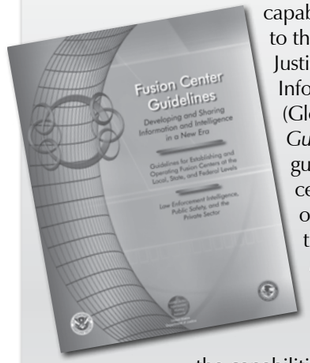
Appendix D: Acronym List 57

Appendix E: Resources 61

Introduction

Purpose

This document identifies the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities. It is an addendum to the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's (Global) *Fusion Center Guidelines,* which provide guidance to ensure that fusion centers are established and operated consistently across the country. Using the *Fusion Center Guidelines,* as well as identified best practices, federal, state, and local officials identified the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions.



By achieving this baseline level of capability, a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information. This baseline level of capability will support specific operational capabilities, such as Suspicious Activity Reporting (SAR); Alerts, Warnings, and Notifications; Risk Assessments; and Situational Awareness Reporting.

The development of baseline operational standards is called for in the *National Strategy for Information Sharing*[1] (Strategy) and is a key step to reaching one of the Strategy's goals: "Establishing a National Integrated Network of State and Major Urban Area Fusion Centers." Defining these operational standards allows federal, state, local, and tribal officials to identify and plan for the resources needed—to include financial, technical assistance, and human support—to achieve the Strategy's goal.

1 The *National Strategy for Information Sharing* was developed in partnership with Global and other state and local officials, to include fusion center officials.

Purpose (continued)

The Strategy recognizes the sovereignty of the state, local, and tribal governments 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 an "all-crimes" approach, whereas others have also included an "all-hazards" approach.[2] The Strategy supports and encourages these approaches, while respecting that a fusion center's mission should be defined based on jurisdictional needs.

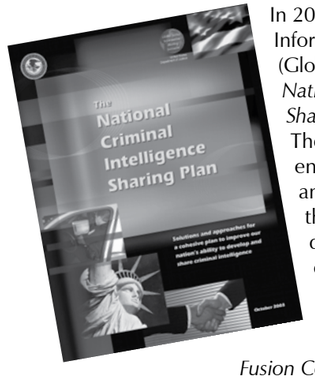
In support of the Strategy's goal, the federal government agreed that a "sustained federal partnership with state and major urban area fusion centers is critical to the safety of our nation, and therefore a national priority." While not all fusion centers receive federal grant funding, most fusion centers receive other types of support from the federal government, including technical assistance, training, colocation of federal personnel, and access to federal information and networks. This document will help the federal government better identify how to support fusion centers. The federal government does not intend to use this document for punitive purposes; rather, a common set of capabilities is needed in order for the U.S. Department of Homeland Security (DHS), DOJ, and other federal agencies to ensure that they are providing the right types of resources in a consistent and appropriate manner. The capabilities also assist in ensuring that fusion centers have the basic foundational elements for integrating into the national Information Sharing Environment.

It is recognized that at the time of writing this document, most fusion centers are in the process of achieving these standards and capabilities. Since resources vary greatly from center to center, it is expected to take a period of one to five years to achieve all of the baseline capabilities. It is also expected that some capabilities may not need to be housed or performed within a fusion center itself; instead, the center may rely on another fusion center or other operational entity to provide the capability. This approach is particularly appropriate, since one of the founding principles of the *Fusion Center Guidelines* is to leverage existing resources and expertise where possible.

2 See Glossary for definition of "all-crimes approach" and "all-hazards approach."

Introduction and Background

Improving information sharing constitutes a cornerstone of our national strategy to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad.

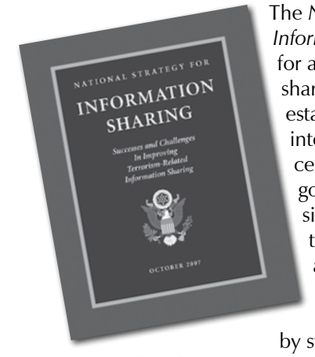


In 2003, DOJ's Global Justice Information Sharing Initiative (Global) developed the *National Criminal Intelligence Sharing Plan* (NCISP).[3] The NCISP provides law enforcement with solutions and approaches to improve the nation's ability to develop and share criminal intelligence. The NCISP provided the foundation for the development of the *Fusion Center Guidelines,* issued in 2006. The *Fusion Center Guidelines*[4] were developed collaboratively between DOJ's Global and DHS's Homeland Security Advisory Council. The purpose of the *Fusion Center Guidelines* is to provide guidance on the establishment and operation of fusion centers at the federal, state, local, and tribal levels.

In 2004, the Information Sharing Environment (ISE) was established by the President and the Congress "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[5] The ISE supports five communities—intelligence, law enforcement, defense, homeland security, and foreign affairs—by leveraging existing capabilities and aligning policies, standards, and systems to ensure that those responsible for combating terrorism have access to timely and accurate information. An improved ISE is being constructed on a foundation of trusted partnerships among federal, state, local, and tribal governments; the private sector; and our foreign allies. Numerous national initiatives have been set forth that provide guidance to the development of the ISE, including the December 2005 Presidential Memorandum, which outlines guidelines and requirements to further the development of the ISE. Many of the results of this Memorandum were incorporated by the Program Manager of the Information Sharing Environment into the *Information Sharing Environment Implementation Plan* issued in November 2006.

3 The NCISP is available at http://it.ojp.gov/documents/NCISP_Plan.pdf.
4 The *Fusion Center Guidelines* document is available at http://it.ojp.gov/documents/fusion_center_guidelines.pdf.
5 Section 1016, Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The IRTPA also established the position of Program Manager for the Information Sharing Environment.

The President's Memorandum is also significant in that it declared for the first time that state and local governments should be treated as full and trusted partners with the federal government in our nation's efforts to combat terrorism.[6] The President directed that a framework be developed to enable that goal, and the results were embraced in the *Information Sharing Environment Implementation Plan* and, most recently, in the President's *National Strategy for Information Sharing* issued in October 2007.



The *National Strategy for Information Sharing* calls for a national information sharing capability through the establishment of a national integrated network of fusion centers. Since 2001, the federal government has provided significant grant funding, training, and technical assistance to support the establishment of fusion centers owned and operated by states and major urban areas.

The Strategy builds on these efforts and provides a federal government-wide approach to interfacing and collaborating with these fusion centers. Additionally, Appendix 1 of the Strategy outlines the federal, state, local, and tribal governments' roles and responsibilities for the establishment and continued operations of state and major urban area fusion centers:

> The roles and responsibilities outlined in the *Strategy* were developed in partnership with state, local, and tribal officials and represent a collective (federal, state, local, and tribal) view. The *Strategy* recognizes the sovereignty of state and local governments, and thus the roles and responsibilities are delineated with the understanding that state and major urban area fusion centers are owned and managed by state and local governments. Furthermore their incorporation into the ISE takes into account that these centers support day-to-day crime control efforts and other critical public safety activities. Interlinking and networking these centers will create a national capacity to gather, process, analyze, and share information. Incorporating these centers into the ISE will be done in a manner that protects the information privacy and other legal rights of Americans and corporations, as provided for under U.S. law. [Appendix 1, Page A-1]

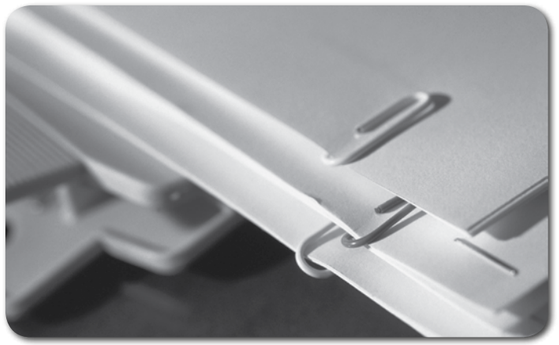
To carry out the roles and responsibilities identified in the Strategy, state and local governments must first define and document how each state intends to carry out intrastate efforts to gather, process, analyze, and disseminate terrorism information, homeland security information, and law enforcement information. This process is commonly known as the "Fusion Process." States with multiple fusion centers will be asked to designate a statewide fusion center to coordinate statewide information sharing efforts. In states with major urban area fusion centers, their activities should be incorporated into the statewide Fusion Process. If the Urban Areas Security Initiative (UASI) does not have a fusion center (referred to as a major urban area), the state's homeland security advisor should work to determine the most effective manner in which to incorporate the UASI into the statewide information sharing framework.

Finally, for local law enforcement or homeland security analysis centers that do not meet a baseline capability definition of a fusion center (and are not in the process of achieving a baseline level of capability), the statewide Fusion Process should incorporate these analysis centers and local law enforcement intelligence capabilities to ensure that information sharing efforts are optimized and barriers minimized. These analysis centers may not possess the ability or may not have the need to establish all of the baseline operational standards and roles and responsibilities as detailed in this document, but they should be incorporated into the state's Fusion Process.

6 Guideline 2, "Guidelines and Requirements in Support of the Information Sharing Environment," Presidential Memorandum of December 16, 2005.

Methodology and Document Structure

Methodology



At the request of the Office of the Program Manager, Information Sharing Environment, DOJ and DHS supported a meeting of subject-matter experts that convened on January 17–19, 2007. The participants represented fusion centers across the country.[7] This group was charged with identifying within the *Fusion Center Guidelines* and other fusion center-related documents those capabilities that should be considered necessary to achieve a baseline operational capability as a fusion center. Additional input was received during subsequent discussions, conference calls, and meetings.

The initial list of baseline capabilities was used for the 2007 Fusion Center Assessment and included in the 2007 and 2008 Homeland Security Grant Program (HSGP) Fusion Capability Planning Tool Supplemental Resource. Given the critical role of the baseline capabilities, it was determined that they would be well suited as an Addendum to the *Fusion Center Guidelines*, and the effort was expanded to provide further explanation on the baseline capabilities and include references, resources, and available best practices to assist with implementation.

In addition to the *Fusion Center Guidelines*, the baseline capabilities and standards outlined in this document were developed using guidance provided in the following national policy documents: the *National Strategy for Information Sharing*, the *National Criminal Intelligence Sharing Plan,* the *Information Sharing Environment Implementation Plan*, and DHS's *National Preparedness Guidelines* and *Target Capabilities List* (TCL) (September 2007).

7 A listing of the Fusion Center Baseline Capability Focus Group participants is contained in Appendix A of this document.

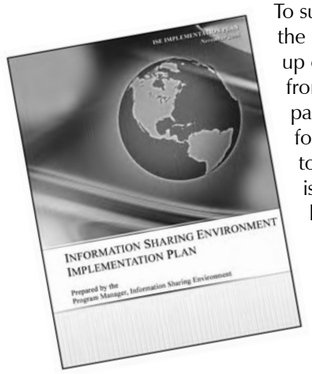
Overview of Comment Adjudication

As a part of the development process, a draft of this document was provided to participants at the 2008 National Fusion Center Conference. Approximately 140 comments or clarifying questions were received, of which more than 75 percent were accepted or addressed in whole or in part. Those that were not accepted usually addressed a section that had been rewritten based on other comments or would have added too much detail for the purposes of this document. A number of comments were broader than a particular capability, providing suggestions affecting the entirety of the document. These broader comments fall into four categories, which are discussed in greater detail below. Accordingly, the document was adjusted to clarify areas of confusion and incorporate suggested changes where possible. Some of these changes include the addition of a section on "How to Use this Document," the consolidation of several categories of the baseline capabilities and reducing many of the standards and tasks under certain capabilities, the addition of a "Privacy" baseline capability category (described below), the addition of capabilities under the Analysis Capability set, and the grouping of the capabilities into two types: (1) those baseline steps which enable the fusion center to conduct each step of the Intelligence Process and (2) those administrative capabilities which enable the proper management and functioning of a fusion center.

Addition of a Set of Privacy-Related Capabilities

During the comment process, the ISE Privacy Guidelines Committee (PGC) reviewed the document and made recommendations to enhance the privacy-related capabilities, in order to assist the incorporation of fusion centers into the Information Sharing Environment. The following information is background on their methodology:

> A core requirement for participation in the Information Sharing Environment (ISE) is that "agencies and the PM-ISE will work with non-federal entities seeking to access or provide protected information through the ISE to ensure that such non-federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those in these Guidelines."[8]



To support this requirement, the ISE PGC, which is made up of ISE Privacy Officials from the federal agencies participating in the ISE, formed a working group to examine the privacy issues relative to state, local, and tribal entities, including fusion centers, interfacing with the ISE. The PGC State/Local/Tribal Working Group (SLT WG) began with the existing guidance found in the *Fusion Center Guidelines*, specifically Guideline 8, "Develop, publish, and adhere to a privacy and civil liberties policy," and performed a gap analysis to identify where the guidance to the fusion centers did not include the requirements of the ISE Privacy Guidelines. While some of the concepts and requirements of the ISE Privacy Guidelines are referenced in Guideline 8, noteworthy gaps were identified, in part because protected information shared in the ISE is given enhanced privacy and civil liberties protection under the ISE Privacy Guidelines. In order to provide the most comprehensive guidance, the gap analysis compares Guideline 8, the ISE Privacy Guidelines, and 28 Code of Federal Regulations (CFR) Part 23, since all address privacy concerns and are relevant to the fusion centers. The gap analysis developed by the SLT WG provides detailed operational guidance that assists fusion centers in formulating their ISE privacy policies.

The PGC's recommendations have been integrated with the privacy-related capabilities, and the resulting capabilities were placed in a new stand-alone category for privacy capabilities. Adherence to these privacy capabilities will ensure that a fusion center's privacy policy is at least as comprehensive as the ISE Privacy Guidelines. The capabilities are keyed to the sections of the ISE Privacy Guidelines, the full text of which can be found at www.ise.gov. As is the case for federal agencies participating in the ISE, each fusion center will need to document its existing policy or establish a new or revised policy or procedure for meeting each baseline requirement. This process will result in a fusion center privacy protection policy that meets the Section 12.d. requirement of the ISE Privacy Guidelines. The Guidelines, along with the *Privacy and Civil Liberties Implementation Guide* (the Guide) and other resource materials on the ISE Web site, should be consulted for details on the ISE Privacy Guidelines requirements that must be addressed in fusion center ISE privacy policies. Further, it is highly recommended that fusion centers also use the Key Issues Guidance papers in the Guide on Redress; Data Quality; Data Security; Notice Mechanisms; and Accountability, Enforcement, and Audit—with special attention to the "core elements" section—in formulating their ISE privacy policies.

In addition to the ISE Privacy Guidelines, the privacy capabilities are based on the requirements laid out in Global's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*. In many cases, the privacy baseline capabilities exceed the requirements of the ISE Privacy Guidelines, because fusion centers address information types and activities that extend beyond the scope of the ISE.

Addition of Capabilities Under the Intelligence Analysis and Production Capability Set

Recognizing that the focus on the analytic components of fusion centers has not been as strong as it needs to be, the International Association of Law Enforcement Intelligence Analysts (IALEIA) provided substantial comments to strengthen this section. They noted that "if we fail in that area, the utility of fusion centers will be in question. Information sharing in and of itself is not a solution to our public safety and homeland security issues." To enhance the Intelligence Analysis and Production capability set, IALEIA suggested capabilities that would strengthen the management of the analytic function, as well as the capabilities of analysts.

8 Section 11 of the Presidentially approved *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines or Guidelines).

General Comments Applying to Whole Document

The general comments typically fell into one of four categories, often with conflicting suggestions. Outlined below are general comments and the resolutions that were incorporated into this document.

1. References to All Crimes, All Hazards in the Baseline Capabilities Document

The nature of the comments revealed different understandings of the terms; therefore, definitions of the all-crimes and all-hazards approaches were added to the Glossary.

Several comments were received regarding the references to "all hazards" in the capabilities. One center suggested that each fusion center or state needs to decide whether to include "all hazards" in its center, and therefore it should not be in this document. Another center suggested that "all hazards" should be the responsibility of emergency management and not a fusion center. Consistent with these comments, the document was adjusted to reflect that the use of an all-hazards approach is not a baseline capability. Instead, the baseline capabilities call for the governance body of the center to take under consideration and make a decision whether it will incorporate an all-crimes and/or all-hazards approach.

As explained in the Purpose section of this document, the *National Strategy for Information Sharing* supports and encourages these approaches, while respecting that a fusion center's mission should be defined based on local needs.

When responding to questions in annual assessments, if a fusion center has decided not to use an all-crimes or all-hazards approach, the center will need to document this decision and its justification.

2. Role of Critical Infrastructure and Key Resources (CIKR) and the Private Sector

Several comments recommended removing references to the private sector; others suggested that support to critical infrastructure and key resource protection activities should not be considered a baseline capability. Accordingly, the document was edited to ensure that the center:

1. Can disseminate alerts, warnings, and notifications and other relevant analytic reports to the affected critical infrastructure or private sector entity; and
2. Has mechanisms in place to receive tips and leads relevant to the center's mission (terrorism, threats, crime, etc.).

The mechanisms used to pass information to and from these entities will vary, and there is no requirement that the fusion center be the "owner" of the information sharing mechanism. If a state or major urban area already has a CIKR information sharing capability that is managed by another organization, the fusion center can simply provide information to that entity as needed. The emphasis in the baseline capabilities is ensuring that these matters have been considered and planned for.

The capabilities also encourage "consideration" of the private sector's input through an Advisory Board or some other mechanism but do not make it a requirement.

For those centers interested in incorporating the support of CIKR into their Fusion Process, an appendix to this document is being developed that will outline the baseline capabilities for a CIKR capability. Please refer to the *Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers (*CIKR Protection Capabilities for Fusion Centers*),* an appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers,* for more information and guidance on the recommended actions necessary to successfully integrate these activities, as well as the resources available to effectively do so. The CIKR Protection Capabilities for Fusion Centers has been jointly developed by the DHS Office of Infrastructure Protection and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) and will be available in fall 2008.

Background on Critical Infrastructure and Key Resources in Homeland Security Preparedness

Efforts to support the protection of CIKR are an essential component of any overarching homeland security program. In accordance with the *National Infrastructure Protection Plan* (NIPP) risk management framework, as well as the benchmarks and requirements identified in the FY2006 and FY2007 HSGP, state governments are responsible for building and sustaining a statewide/regional CIKR protection program. This program must include the processes necessary to implement the NIPP risk management framework at the state and/or regional level, including urban areas, as a component of the state's overarching homeland security program.

Additionally, the national priorities identified in the *National Preparedness Guidelines* help guide the nation's preparedness efforts to meet its most urgent needs. With the inclusion of NIPP[9] implementation as one of these

9 The NIPP is the comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies, and tribal partners. The NIPP lays out the plan for setting requirements for infrastructure protection, which will help ensure our government, economy, and public services continue in the event of a terrorist attack or other disaster. The NIPP was released on June 30, 2006. The purpose of the NIPP is to "build a safer, more secure, and more resilient America by enhancing protection of the nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."

overarching national priorities, CIKR protection programs form an essential component of state, territorial, local, tribal, and sector-specific homeland security strategies. Achieving that national priority requires meeting objectives that include understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. To achieve these efforts, CIKR security partners should have the following:

- Coordinated, risk-based CIKR plans and programs in place addressing known and potential threats;
- Structures and processes that are flexible and adaptable, both to incorporate operational lessons learned and effective practices and also to adapt quickly to a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information sharing networks that include relevant intelligence, threat analysis, and real-time incident reporting.[10]

These objectives are inherent in the information sharing and intelligence cycle processes that occur within fusion centers on a daily basis, and therefore there is a natural tendency for fusion centers and CIKR protection programs to coordinate and integrate their efforts so that they can more successfully leverage resources and integrate the gathering, analysis, and sharing of CIKR-related information and intelligence with all other threat information, whether criminal, homeland security, or counterterrorism in nature. The coordination and integration of these efforts also support achievement of the Expand Regional Collaboration and Strengthen Information Sharing and Collaboration national priorities noted in the *National Preparedness Guidelines*.

Therefore, fusion centers are strongly encouraged to consider the integration of federal, state, local, and private sector CIKR protection efforts in their current operational capabilities. The integration of CIKR capabilities should not be separated from all other ongoing intelligence and information sharing activities, but rather the CIKR capabilities should be integrated throughout every step of the intelligence process. This will ensure that CIKR information is appropriately coordinated and integrated with other federal, state, local, and private sector threat information, whether criminal, homeland security, or counterterrorism in nature. The incorporation of CIKR-related information throughout the intelligence processes occurring in the fusion center will provide a more comprehensive understanding of the threat, vulnerabilities, potential consequences of attacks, and the effects of risk-mitigation actions. It will also allow fusion centers to more successfully plan for and support the development of preventive and protective measures to deter, disrupt, and/or mitigate threats.

3. Concerns of Rural/Small States

Several fusion centers indicated concerns that the baseline capabilities would not be achievable for those fusion centers with one or two staff members and limited budgets. As noted in the Background section, it is expected that there will be local law enforcement or homeland security analysis centers that may not possess the ability or may not have the need to establish all of the baseline operational standards and roles and responsibilities as detailed in this document. Though these entities may not be considered fusion centers, they are an important part of the Fusion Process and should be incorporated into the statewide Fusion Process to ensure that information sharing efforts are optimized and barriers minimized.

In the few cases in which a state's center does not intend to meet the baseline capabilities definition of a fusion center, it is important to note that the capabilities performed through an intelligence unit or analysis center are considered important components of the national Fusion Process. These states should consider partnering with an adjacent state's fusion center and ensure appropriate connectivity with federal partners and other regionally based information sharing systems.

4. Suggestions to Tier Baseline Capabilities

Suggestions were made to tier the capabilities. During revisions, efforts were made to scale back or consolidate the details of the capabilities. As noted above, it is recognized that the application of these capabilities will vary depending on the unique environment in which the fusion center operates. However, a common definition is needed to support the development of an assessment and resource process that will support fusion centers. Therefore, it was determined that this document would remain focused on one set of baseline capabilities needed to operate a fusion center successfully.

It is expected that each center will need to evaluate these capabilities and determine whether they apply within its unique environment. It is also expected that some capabilities may not need to be housed or performed within a fusion center itself; instead, the center may rely on another fusion center or other operational entity to provide the capability. That is particularly appropriate, since one of the founding principles of the *Fusion Center Guidelines* is to leverage existing resources and expertise where possible.

10 See *National Preparedness Guidelines*.

Future Versions

This report should be viewed as a "living document" and will be periodically updated. Those charged with developing and implementing the baseline capabilities will continue to solicit input on improving fusion center operations from law enforcement and homeland security communities, national organizations, and other government and public safety entities. Individuals and organizations are invited to submit recommendations and comments regarding this document via the National Criminal Intelligence Resource Center (http://www.ncirc.gov) e-mail address: information@ncirc.gov.

The Baseline Capabilities Are in Two Sections

I. Fusion Process Capabilities

These capabilities outline those standards necessary to perform the steps of the Intelligence Process within a fusion center. These areas are:

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

II. Management and Administrative Capabilities

These capabilities enable the proper management and functioning of a fusion center. These areas are:

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

Document Structure and Use

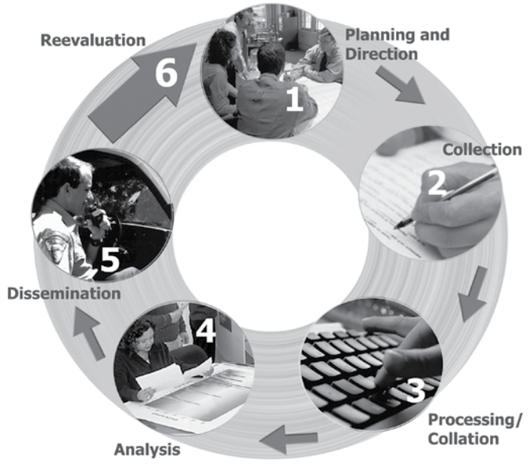
Document Organization

The baseline capabilities are organized into two sections: I. Fusion Process Capabilities—which outline those standards necessary to perform the steps of the Intelligence Process within a fusion center, and II. Management and Administrative Capabilities—which enable the proper management and functioning of a fusion center.

For the purposes of this document, the steps of the Intelligence Process provide the foundation of the capabilities needed to perform the Fusion Process. For example, step one of the Intelligence Process is "Planning and Direction," which involves identifying the need for data; agencies should engage in a process of deciding what they want to know before they collect it.[11] Similarly, fusion centers should engage in a planning and coordination step when determining the types of information they should collect, including suspicious activity; alerts, warnings, and notifications; and situational awareness information. While it is acknowledged that the Intelligence Process is different from the Fusion Process, the basic foundational steps of the Intelligence Process can be applied to identifying the baseline capabilities fusion centers should strive to achieve in regards to information and intelligence collection, collation, analysis, and dissemination.

The Intelligence Process is defined in the NCISP and incorporated into Guideline 1 of the *Fusion Center Guidelines*.

The Intelligence Process



11 *Fusion Center Guidelines*, p. 20.

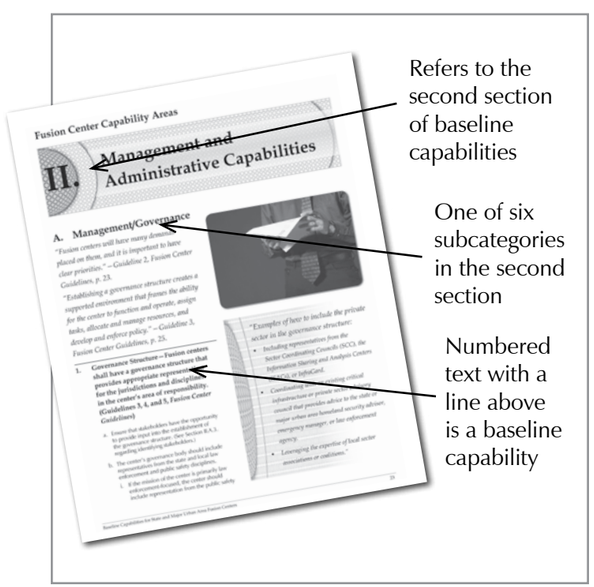
For purposes of baseline capabilities, the Fusion Process capability areas are modified to be:

1. Fusion Process Capabilities:
    - Planning and Requirements Development
    - Information Gathering/Collection and Recognition of Indicators and Warnings
    - Processing and Collation of Information
    - Intelligence Analysis and Production
    - Intelligence/Information Dissemination
    - Reevaluation

2. Management and Administrative Capabilities:
    - Management/Governance
    - Information Privacy Protections
    - Security
    - Personnel and Training
    - Information Technology/Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure
    - Funding

How to Read the Baseline Capabilities

Each of the 12 capability areas identifies the baseline capabilities and standards or tasks necessary to achieve the capability. This document does not prescribe the method of implementation; instead, it provides references to existing and forthcoming documents that describe best practices and guidance on implementation (e.g., the *Fusion Center Guidelines*, the NCISP, and Global's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*).



A consolidated list of these references is included in Appendix E.

Each capability either draws from or builds on one or a few of the *Fusion Center Guidelines*. For ease of reference, each capability highlights the most relevant guidelines.

Suggestions, notes, and examples are included in text boxes to the side, top, or bottom of the capabilities. If the term "consider" or "consideration" is used, the text thereafter should be read as a strong suggestion but not a required baseline capability.

How to Use This Document

This document is designed to be used by fusion center managers, staff, and stakeholders, as well as state and local executive and legislative officials with oversight and budgetary responsibilities, for the purpose of assisting in the identification, prioritization, and allocation of resources to achieve baseline levels of capability based on locally identified needs.

It will be valuable for state and major urban area fusion centers to take into account the capabilities they have achieved, as well as identify capability gaps and the plans to mitigate those gaps, when preparing funding requests and investment justifications (e.g., DHS and DOJ grant funds, as well as state and local funding).

Likewise, this document will help the federal government identify how to support fusion centers through training, technical assistance, human resources, access to information, and grant funds in a consistent and appropriate manner. The federal government intends to update its annual fusion center assessment to reflect this version of the baseline capabilities. This will allow for a greater understanding of the current capabilities and capacity that exist at regional and national levels and enable the federal government to target resources to ensure that capabilities are achieved and sustained.

As noted in the Purpose and Methodology sections, there will be instances in which a capability is not needed at the fusion center because it is either outside the scope of the center's mission or is already addressed by another agency. When responding to questions in future annual assessments, if a fusion center lacks a particular capability and the capability is not under development or being planned for, the center will need to document the reason why it will not house the capability and—as appropriate to the question—identify whether any other outside state or local agency might be addressing the capability.

Fusion Center Capability Areas

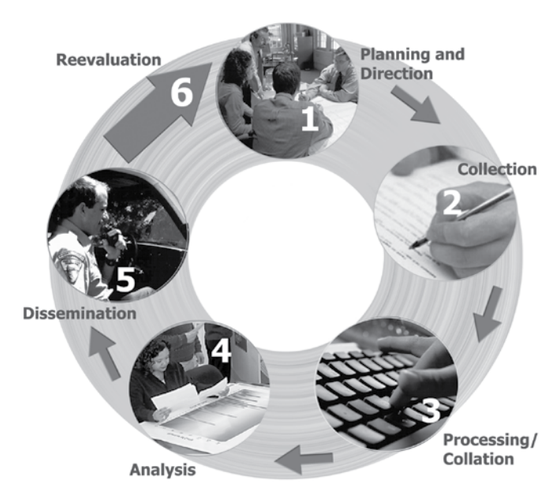
I. Fusion Process Capabilities

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

Guideline 1, Fusion Center Guidelines.

The Fusion Process capabilities identify those capabilities and standards necessary to perform the steps of the Intelligence Process within a fusion center, including the gathering, analysis, and dissemination of information and intelligence. Though the steps and actions of the Fusion Process do not comprehensively mirror the steps of the Intelligence Process, the Intelligence Process provides the foundation to carry out the Fusion Process and assist in the identification of the capabilities needed to successfully complete the Fusion Process.

The Intelligence Process



The Intelligence Process is defined in the NCISP and incorporated into Guideline 1 of the *Fusion Center Guidelines*.

For purposes of baseline capabilities, the Fusion Process capability areas are modified to be:

- Planning and Requirements Development
- Information Gathering/Collection and Recognition of Indicators and Warnings
- Processing and Collation of Information
- Intelligence Analysis and Production
- Intelligence/Information Dissemination
- Reevaluation

The following capabilities address the plans and their associated policies, standards, processes, and procedures (collectively "procedures") needed to perform various aspects of the Fusion Process: the gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information. For these capabilities to be considered achieved or accomplished, the plans and procedures should be documented and provided to appropriate center personnel and partners. Though the types of plans and procedures are broken down by topic, they are in practice integrated aspects of the Fusion Process; therefore, many of these plans should be developed concurrently to the extent possible. In many cases, the resulting plans and procedures may not be separate documents but may be individual components of a larger document, such as a center's Concept of Operations, Standard Operating Procedures, or Policies and Procedures Manual.

The following capabilities do not include capabilities that are otherwise addressed in Section II. Management and Administrative Capabilities (e.g., Information Privacy Protections, Security, Information Technology).

A. Planning and Requirements Development

The Planning and Requirements Development stage "lays the foundation for the types of information that will be collected."
– Guideline 1, Fusion Center Guidelines, p. 21.

1. Intrastate Coordination – In developing and implementing all Fusion Process-related plans and procedures, the center shall coordinate with other fusion centers (the designated state fusion center and/or any UASI fusion center(s)) within its state to identify the roles and responsibilities of each center in carrying out the Fusion Process (gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information) on a statewide basis.

a. Identify and incorporate local and tribal law enforcement, homeland security, or other discipline analytic centers that do not meet the definition of a fusion center but are within the fusion center's geographic area of responsibility, and develop and maintain coordination procedures and communication methodologies.

b. The plan should address the further dissemination of federally generated alert, warning, and notification messages, bulletins, and situational reports, including the identification and establishment of a communications platform to support the timely dissemination of these products.

c. The plan should clearly identify who is responsible for disseminating what types of products and to whom (which local, tribal, and federal authorities; the private sector; and the general public, as appropriate), in order to reduce duplicative dissemination to the extent possible.

2. Risk Assessment – Fusion centers shall conduct or contribute to a statewide and/or regional risk assessment that identifies and prioritizes threats, vulnerabilities, and consequences at regular intervals.

a. Use available national and statewide risk assessments and other relevant products that identify patterns and trends reflective of emerging threats in the development of statewide and regional risk assessments.

b. Develop site-specific and topical risk assessments as appropriate.

c. Provide the risk assessment or a summary and/or briefings on the risk assessment to law enforcement and homeland security officials with planning, resource allocation, and budgeting responsibilities, including appropriate elected officials from the executive and legislative branches.

d. Maintain mechanisms to contribute information of value to other state, multistate, and national-level risk assessments.

3. Information Requirements – The information requirements for the fusion center shall be defined, documented, updated regularly, and consistent with the center's goals and objectives as defined by the governance structure and reflect the risks identified in the statewide and/or regional risk assessment.

a. Use the risk assessment to identify and prioritize the information requirements in order to address the risks (threats, vulnerabilities, and consequences) posed in the center's geographic area of responsibility.

b. Create a formal process to define, communicate, and modify intelligence requirements and intelligence gathering.

c. Establish goals and objectives for collecting, producing, and sharing information.

d. Review and consider including relevant requirements from the national intelligence requirements as provided by DHS and the Federal Bureau of Investigation (FBI).

e. Coordinate with the state and major urban area homeland security advisors and the DHS Protective Security Advisor(s) to ensure coordination and support of the *National Infrastructure Protection Plan* (NIPP).

f. Coordinate information requirements with other interested agencies (local FBI Field Intelligence Group [FIG], Joint Terrorism Task Forces [JTTF], High Intensity Drug Trafficking Areas [HIDTA], etc.) as appropriate.

4. Suspicious Activity Reporting (SAR) – Fusion centers shall develop, implement, and maintain a plan to support the establishment of a suspicious activity and incident reporting process for their geographic area of responsibility, in a manner consistent with the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project.*[12] Specifically, centers shall have the ability to receive, process, document, analyze, and share SARs in a manner that complies with the ISE-SAR Functional Standard.[13]

a. Adhere to the state and local responsibilities for SARs outlined in Appendix 1 of the *National Strategy for Information Sharing* (page A1-6).

b. The fusion center's SAR process should complement and support the SAR processes established or being established by state or local law enforcement agencies within the fusion center's geographic area of responsibility.

c. In cooperation with state or local law enforcement agencies within the fusion center's geographic area of responsibility that have developed or are developing a SAR process, the fusion center shall support:
   i. Defining and documenting the process to be used by the originating agency to ensure that suspicious activity reporting is made available to fusion centers and local JTTFs in a timely manner.
   ii. Developing outreach material for first responders, public safety, and private sector partners and the public to educate them on recognizing and reporting behaviors and incidents indicative of criminal activity associated with international and domestic terrorism.

d. The fusion center, in the absence of a specified threat or risk, should utilize SARs to analyze data trends and identify any potential terrorism linkage or activity (including precursor activity) and disseminate to the JTTF and other appropriate federal, state, and/or local entities.

e. The designated statewide fusion center shall coordinate an effort or support existing efforts to identify system requirements for the state's designated shared space[14] that will support

12 The Major Cities Chiefs Association, Global, DOJ, and DHS supported the development of this report, which describes "the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity by the local police agency."

13 For additional information regarding the ISE Functional Standard for SAR, visit http://www.ise.gov/pages/ctiss.html.

14 The ISE Shared Spaces concept is a key element of the *ISE Enterprise Architecture Framework* and helps resolve the information processing and usage problems identified by the 9/11 Commission. ISE Shared Spaces are networked data and information repositories used by ISE participants to make their standardized terrorism-related information, applications, and services accessible to other ISE participants. ISE Shared Spaces also provide an infrastructure solution for those ISE participants with national security system (NSS) network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Additionally, ISE Shared Spaces also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts. For more information about the ISE Shared Spaces concept, reference the *ISE Enterprise Architecture Framework* and the *ISE Profile Architecture Implementation Strategy* at www.ise.gov.

statewide reporting, tracking, and accessing of SARs in a manner that ensures consistent use of data elements and collection procedures. (Refer to Section II.E. Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure; the ISE-SAR Functional Standard; and the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*.)

f. Fusion centers should support or develop training for law enforcement and nontraditional partners to identify and appropriately report suspicious activities, indicators, and warnings.

5. Alerts, Warnings, and Notifications—Fusion centers shall ensure that alerts, warnings, and notifications are disseminated, as appropriate, to state, local, and tribal authorities; the private sector; and the general public.

a. Fusion centers shall develop and implement a written policy outlining standard operating procedures to govern the receipt of further dissemination of federally generated alert, warning, and notification messages, consistent with the intrastate coordination plan called for by Section I.A.1.

b. In response to federally generated alert, warning, and notification messages and/or significant events, the fusion center shall support or facilitate the identification of actions that were taken by state, local, and tribal authorities and the private sector and report those back to the appropriate federal agency.

c. Adhere to the state and local responsibilities for alerts, warnings, and notifications outlined in Appendix 1 of the *National Strategy for Information Sharing* (page A1-8).

6. Situational Awareness Reporting—Fusion centers shall develop processes to manage the reporting to key officials and the public of information regarding significant events (local, regional, national, and international) that may influence state or local security conditions.

a. Fusion centers shall develop and implement a written policy outlining standard operating procedures to govern the receipt and further dissemination of federally generated information bulletins and other situational awareness messages, consistent with the intrastate coordination plan called for by Section I.A.1.

b. Adhere to the state and local responsibilities for situational awareness reporting outlined in Appendix 1 of the *National Strategy for Information Sharing* (page A1-9).

7. Data Sources—Fusion centers shall identify and document data sources and repositories needed to conduct analysis based on the mission of the center, the findings of the Risk Assessment, and the center's defined Information Requirements.

a. Refer to Section II.E. Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure to further develop plans for access to data sources based on the fusion center's defined mission and core business processes.

8. Coordination With Response and Recovery Officials—Fusion centers shall identify and coordinate with emergency managers and appropriate response and recovery personnel and operations centers to develop, implement, and maintain a plan and procedures to ensure a common understanding of roles and responsibilities and to ensure that 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).

b. The plan should identify roles, responsibilities, and protocols to govern the timely reporting of significant events occurring within state or local jurisdictions to federal authorities and, when appropriate, other states, localities, or regional entities.

c. Ensure that the plan addresses the contingency and continuity-of-operations (COOP) planning during an emergency. (See Section II.E.)

9. Coordination With Private Sector and Critical Infrastructure and Key Resources (CIKR) Information Sharing—Fusion centers, in partnership with locally based federal authorities, shall develop, implement, and maintain a plan and procedures for sharing information with owners of CIKR and, in general, the private sector, in a coordinated manner.

a. All centers shall include in the plan the procedures to disseminate alerts, warnings, and notifications and other relevant analytic reports to critical infrastructure sectors and/or private sector entities that are affected by the threat.

b. The plan should document the decision of the center's governance structure—based on the center's mission, risk assessment, and information requirements—whether the center will establish a CIKR capability to integrate and analyze threat, vulnerability, and consequence data and enable and support state, local, and private sector decision making and activities to protect CIKR.

Note: At a minimum, the baseline capabilities require fusion centers to have the capability to receive information from the private sector and disseminate critical information to members of the private sector. Beyond those baseline capabilities, some fusion centers are encouraged, but not required, to incorporate the needs of the CIKR protection activities into their Fusion Process. This option should be considered by the governance structure as a part of the mission development process. (See Section II.A.)

References: For those centers interested in incorporating the support of CIKR into their Fusion Process, an appendix to this document is being developed that will outline the fusion center capabilities for supporting CIKR protection activities.

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

a. Exercises should include simulations, games, tabletops, functional exercises, and full-scale field exercises.

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.

c. Centers should use the exercises to validate center operations, policies and procedures, and training activities and develop action plans to mitigate any identified gaps.

B. Information Gathering/ Collection and Recognition of Indicators and Warnings

"The stage in which the planning and requirements development stage becomes operational…information is collected from various sources, including law enforcement agencies, public safety agencies, and the private sector. This stage is essential for fusion centers to be effective." – Guideline 1, Fusion Center Guidelines, p. 21.

1. Information-Gathering and -Reporting Strategy – Fusion centers shall develop, implement, and maintain an information-gathering and -reporting strategy that leverages existing capabilities and shall identify methods for communicating information requirements and the overall information-gathering strategy to partners, to include any applicable fusion liaison officers.

a. Clearly outline the collection process, including how the collectors of information are identified and tasked—or if the center lacks the authority to task, identify how such requests are made to partners.

b. Leverage and/or coordinate with the JTTF and other federal, state, local, tribal and private sector information sharing and counterterrorism efforts.

c. Clearly outline the processes that partner organizations—including law enforcement, public safety, private organizations, and the public—use to report information to the fusion center.

d. The strategy and associated processes shall be consistent with the governance structure's defined, agreed-upon, and auditable privacy policy. (Reference Section II.B.)

2. Feedback Mechanism – Fusion centers shall define and implement a feedback mechanism that:

a. Provides the reporting entity an acknowledgement of the receipt of its information and, to the extent possible, provides feedback on the value of the information and actions taken with the information.

b. Allows collectors to make suggestions to improve the strategy, plans, or processes, as well as seek clarification on information requirements.

c. Allows recipients of information or products to make suggestions to improve products.

3. Collection and Storage of Information – Fusion centers shall define the policies and processes and establish a mechanism for receiving, cataloging, and retaining information provided to the center.

a. Ensure that policies, processes, and mechanisms comply with the center's privacy policy—particularly regarding data retention, purging, and redress. (Reference Section II.B.)

b. Fusion centers should reference the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 regarding intelligence collection and the types of information to collect, methods for purging out-of-date or incorrect information, and procedures for the utilization of intelligence personnel and techniques.[15]

c. Adhere to the Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines*[16] and the LEIU *Audit Checklist for the Criminal Intelligence Function*[17] for the maintenance of criminal intelligence files.

d. Adhere to the collection, storage, and retention requirements of 28 CFR Part 23.

e. Establish processes to routinely identify progress achieved against individual information requirements and the overall information-gathering strategy, and provide summary assessments to fusion center partners, management, and the governance body on a routine basis.

f. The mechanism used to catalog and retain information shall enable timely retrieval by the center's analysts.

g. Develop protocols to ensure the archiving of all appropriate data, information, and intelligence to support future efforts.

h. To the extent the processes and mechanisms are automated, adhere to the Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure capabilities. (Section II.E.)

15 Additional information regarding CALEA Standard 51.1.1—Criminal Intelligence is available at http://www.calea.org/online/newsletter/no79/criminalintelligence.htm.
16 LEIU *Criminal Intelligence File Guidelines*—http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

C. Processing and Collation of Information

"Processing and collation involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined." – Guideline 1, Fusion Center Guidelines, p. 20.

1. Information Collation – Fusion center analysts shall use the necessary and available tools to process and collate information and intelligence to assist with accurate and timely analysis.

a. Fusion center analysts should consider utilizing the appropriate tools identified in Global's *Analyst Toolbox* to assist in the collation of information.

b. Fusion center analysts should reference IALEIA and Global's *Law Enforcement Analytic Standards* when developing the processes for collating information.

c. Fusion centers should consider the development or utilization of an intelligence collection system that allows for the collection, processing, collation, and storage of information related to the mission of the center.

2. Levels of Confidence – Fusion centers shall liaise with partners to ensure that information collected is relevant, valid, and reliable.

a. Fusion center personnel should consider regular meetings with information providers to discuss information collection requirements.

b. Fusion center personnel should ensure that partners are aware of the various levels of confidence of information provided to the center.

i. 28 CFR Part 23 states, "Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and officers."

ii. Levels of confidence relate to reliability, validity, and relevancy.

17 LEIU *Audit Checklist for the Criminal Intelligence Function*—http://it.ojp.gov/documents/LEIU_audit_checklist.pdf.

D. Intelligence Analysis and Production

"Analysis transforms the raw data into products that are useful…the goal is to develop a report that connects information in a logical and meaningful manner to produce an intelligence report that contains valid judgments based on analyzed information. …One of the goals of the fusion center during this stage is to identify trends or information that will prevent a terrorist attack or other criminal activity."
– Guideline 1, Fusion Center Guidelines, pp. 20–21.

1. Analytic Products—Fusion centers shall develop, implement, and maintain a production plan that describes the types of analysis and products they intend to provide for their customers and partners (which, at a minimum, include Risk Assessments; Suspicious Activity Reporting; Alerts, Warnings, and Notifications; and Situational Awareness Reporting [see Sections I.A.2, 4, 5, and 6 for further details on these product types]), how often or in what circumstances the product will be produced, and how each product type will be disseminated.

a. Adhere to the tenets in IALEIA and Global's *Law Enforcement Analytic Standards* booklet,[18] particularly Standards 17, 20, and 21, which address Analytic Product Content, Report, and Format standards.

b. The production plan shall be prioritized based on the center's mission, information requirements, and priority functions.

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.

2. Fusion Process Management—An intelligence commander/manager should be designated to oversee the management of the Fusion Process (including the collection, collation, analytic function, dissemination, and reevaluation of information and intelligence) within the center.

a. The commander/manager should address the day-to-day intelligence management functions of the center.

b. The commander/manager should prioritize critical intelligence products and ensure that the critical outputs of the fusion center are accomplished.

c. The commander/manager should have the necessary skill sets to oversee the production of intelligence products that are effective, efficient, and permissible under state and federal laws and regulations.

d. The commander/manager should have previous experience and management training.

   i. Training should include the intelligence cycle, analytical training, intelligence management, the role of the fusion center, and legal issues.

18 IALEIA and Global's *Law Enforcement Analytic Standards* booklet is available at http://www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf.

3. Enhancing Analyst Skills—The fusion center should develop and implement a Training and Professional Development Plan to enhance analysts' critical thinking, research, writing, presentation, and reporting skills.

a. The supervisor of the analytic function should work with each analyst to draft a Training and Professional Development Plan. Components of the plan should include training and mentoring opportunities for learning new subject matter/areas of expertise and exposure to new analytic techniques and technologies.

   i. The initial training goal should be the completion of the Foundations of Intelligence Analysis Training program or its training equivalent and the certification of analysts.

   ii. Adhere to the tenets in IALEIA and Global's *Law Enforcement Analytic Standards* booklet,[19] particularly Standards 1–7 for analysts.

   iii. Utilize IALEIA and Global's *Law Enforcement Analytic Standards* and the *National Criminal Intelligence Sharing Plan* in the development of the training plan.

b. Analysts should be provided routine opportunities to present their analytic findings and receive feedback on the quality of their written reports and oral presentations.

c. Performance evaluations should be conducted at least annually, and the Training and Professional Development Plan updated accordingly.

4. Information Linking—Fusion centers shall ensure that analysts are able to understand and identify the links between terrorism-related intelligence and information related to traditional criminal activity so they can identify activities that are indicative of precursor behaviors, terrorist activities, and threats. (Guidelines 12, 13, 14, *Fusion Center Guidelines*)

a. Training regarding precursor activities of terrorists should be provided to analysts and relevant fusion center personnel following the standards outlined in the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*.[20]

b. Ensure that analysts receive training on the analytic process, analytical writing and briefing skills, and reporting skills.

5. Strategic Analysis Services—Fusion centers shall develop the capability to provide strategic analysis services for the jurisdiction served. (Guideline 14, *Fusion Center Guidelines*.)

6. Open Source Analysis Capability—Fusion centers shall establish an open source analysis capability utilizing the free training and tools provided by the federal government.

7. Analyst Specialization—Fusion centers should assign "accounts" or "specialties" to analysts based on the priorities of the fusion center, to allow the development of analytic depth.

8. Analytical Tools—Fusion centers shall provide the necessary tools to analysts for the analysis of information and data. (Guidelines 11 and 14, *Fusion Center Guidelines*)

a. Fusion centers should provide all tools outlined in Global's *Analyst Toolbox* document.

b. Training should be provided for the identified analytic tools so that relevant personnel are proficient in their use.

c. Analysts shall be provided with routine mechanisms to communicate with other fusion center analysts within the state or region. (Examples include "chat rooms" available via Homeland Security State and Local Intelligence Community of Interest [HS SLIC] or other collaborative networks or regular phone calls.)

d. Analysts shall have access to and understanding of where to find information sources and available expertise to support the information priorities of the fusion center.

19 IALEIA and Global's *Law Enforcement Analytic Standards* booklet is available at http://www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf

20 The *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* is accessible at http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf.

E. Intelligence/Information Dissemination

"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" – Definition of Dissemination, Criminal Intelligence Glossary.

1. Dissemination Plan – Fusion centers shall develop a high-level dissemination plan that documents the procedures and communication mechanisms for the timely dissemination of the center's various products to the core and ad hoc customers.

a. The plan should be consistent with the intrastate coordination plan. (See Section I.A.1.)

b. Consider a variety of methods to distribute information, including Web site; e-mail; secure portal; regional and national information sharing systems such as Regional Information Sharing Systems® (RISS), Homeland Security Information Network (HSIN), Law Enforcement Online (LEO), and HS SLIC; pager; fax; telephone; video teleconferencing system; and personal contact. (Reference Guideline 6, *Fusion Center Guidelines*, for further suggestions.)

2. Reporting of Information to Other Centers – Fusion centers shall develop the processes and protocols for ensuring that relevant and vetted priority information is reported to fusion centers in other states and localities to support regional trends analysis. (Guideline 7, *Fusion Center Guidelines*)

3. Reporting of Information to Federal Partners – Fusion centers shall develop the processes and protocols, in coordination with the FBI and DHS Office of Intelligence and Analysis (I&A), for ensuring that relevant and vetted priority information is reported to the JTTF and other appropriate federal agencies to support its inclusion into national patterns and trends analysis.

a. In addition to the priority information processes (SAR; Alerts, Warnings, and Notifications; and Situational Awareness Reporting), share information to address national security and criminal investigations.

b. Ensure that information provided to the federal government is shared according to the fusion center's privacy policy. (See Section II.B.)

c. Utilize the protocols established in the SAR report, National Information Exchange Model (NIEM), and Information Exchange Package Documents for information exchange.

F. Reevaluation

"Reevaluation assesses current and new information, assists in developing an awareness of possible weak areas as well as potential threats, and strives to eliminate previously identified weaknesses that have been hardened as a result of the Fusion Process. Overall, this step provides an opportunity to review the performance or effectiveness of the fusion center's intelligence function." – Guideline 1, Fusion Center Guidelines, p. 20.

1. Performance Evaluation – Fusion centers shall develop and implement a plan to reevaluate the center's performance of the intelligence cycle on a regular basis.

a. Develop mechanisms to receive stakeholder feedback on all parts of the intelligence cycle.

b. Incorporate feedback from training and exercises.

c. Update plans and procedures as appropriate.

2. Fusion Center Processes Review – Fusion centers shall establish a process to review and, as appropriate, update the center's information requirements, collection plan, and analytic production strategy on a regular basis and any time one of the following is received:

a. New threat or vulnerability information;

b. New federal or state standing or ad hoc information requirements;

c. Federal or state alerts, warnings, or notifications or situational awareness bulletins; and/or

d. Updated risk assessment.

II. Management and Administrative Capabilities

A. Management/Governance

"Fusion centers will have many demands placed on them, and it is important to have clear priorities." – Guideline 2, Fusion Center Guidelines, p. 23.

"Establishing a governance structure creates a supported environment that frames the ability for the center to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy." – Guideline 3, Fusion Center Guidelines, p. 25.

1. Governance Structure—Fusion centers shall have a governance structure that provides appropriate representation for the jurisdictions and disciplines in the center's area of responsibility. (Guidelines 3, 4, and 5, *Fusion Center Guidelines*)

a. Ensure that stakeholders have the opportunity to provide input into the establishment of the governance structure. (See Section II.A.3. regarding identifying stakeholders.)

b. The center's governance body should include representatives from the state and local law enforcement and public safety disciplines.

   i. If the mission of the center is primarily law enforcement-focused, the center should include representation from the public safety

"Examples of how to include the private sector in the governance structure:

- *Including representatives from the Sector Coordinating Councils (SCC), the Information Sharing and Analysis Centers (ISACs), or InfraGard.*
- *Coordinating with an existing critical infrastructure or private sector advisory council that provides advice to the state or major urban area homeland security advisor, emergency manager, or law enforcement agency.*
- *Leveraging the expertise of local sector associations or coalitions."*

discipline in at least an advisory capacity. This will enhance the center's ability to perform key baseline capabilities, including:

a) Receiving tips from and disseminating alerts, warnings, notifications, and relevant analytic products to public safety organizations; and
b) Supporting emergency management, response, and recovery planning activities based on likely threat scenarios and at-risk targets.

c. The center's governance body should include representatives from the federal government in at least an advisory capacity.

i. Include local representatives from the FBI (i.e., the JTTF and FIG) and appropriate components of DHS (i.e., Protective Security Advisor, U.S. Coast Guard, Federal Emergency Management Agency [FEMA], U.S. Immigration and Customs Enforcement [ICE], United States Secret Service [USSS], etc.).

ii. Also consider including or coordinating with the following efforts as appropriate to the center's mission and location: HIDTAs and the U.S. Attorney's Office's Anti-Terrorism Advisory Council (ATAC).

d. Consideration should be given to include the perspectives of the private sector, where appropriate, in at least an advisory capacity.

e. Ensure that the governance body is composed of officials with decision-making authority, capable of committing resources and personnel to the center.

f. Ensure that bylaws for the operations of the governance structure are developed and adopted by the governance body.

g. The governance body shall clearly define the management and command structure of the center.

h. The governance body should develop and approve key fusion center policies, including the center's privacy and security policies. (See Sections II.B. and C. for more information on Information Privacy Protections and Security capabilities).

i. The governance body shall receive at least annual reports on the center's compliance with the defined privacy and security policies.

j. Develop communication mechanisms to provide the governance body with feedback from center management and personnel, stakeholders, and recipients of information within the state or region.

k. The governance body should include representation from and ensure that the fusion center management coordinates with other fusion centers within the state (the designated state fusion center and/or any UASI fusion center(s)), in order to identify the roles and responsibilities of each center in carrying out the Fusion Process (gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information) on a statewide basis.

l. Review the governance structure and membership at regular intervals to determine whether additional organizations or disciplines should be included based on the current risk assessment and the fusion center's mission.

2. Mission Statement—Fusion centers shall have a defined mission statement that is clear and concise and conveys the purpose, priority, and roles of the center. (Guideline 2, *Fusion Center Guidelines*)

a. The governance body shall develop and adopt the mission statement, unless it has been predefined by law or executive order.

b. In defining the mission statement, consideration should be given to the risks identified in the center's geographic area of responsibility.

c. In defining the mission statement, the governance body should consider using an all-crimes approach and/or an all-hazards approach (see Glossary for definition of these terms), recognizing that precursor crimes or incidents may have national security implications.

i. If the governance body determines that the center will incorporate certain public safety disciplines into the fusion center's mission and/or determines the center will use an all-hazards approach, centers shall adhere to the forthcoming appendices to this document, which will outline the baseline capabilities for incorporating the following disciplines into the center:
a) Fire Service
b) Public Health
c) Critical Infrastructure and Key Resources

ii. If the fusion center utilizes an all-crimes approach, the center should liaise with applicable agency and multijurisdictional task forces and intelligence units, including:
a) Gang task forces and intelligence units, as well as the National Gang Intelligence Center (NGIC)[21]
b) Narcotic-related task forces and intelligence units, as well as the National Drug Intelligence Center (NDIC)
c) Violent crime/fugitive task forces and intelligence units
d) Economic crime task forces and intelligence units

d. The governance body shall provide oversight to ensure that the mission statement, the most recent risk assessment, and the identified customer needs inform the Planning and Requirements Development process. (See Section I.A., particularly the prioritizing of fusion center functions and tasks.)

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*)

a. Review the most recent risk assessment, if available, and identify relevant stakeholders that should be included to address the highest identified risks.

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.

c. When identifying the roles and responsibilities of core and ad hoc stakeholders, identify their needs as a customer of the center, as well as their contributions to the center (for example: providing resources such as funding, personnel, and access to expertise or providing access to information or databases).

d. After a governance structure has been established and a mission statement approved, review the identified stakeholders and their roles and responsibilities to determine whether any additional organizations should be included or whether roles and responsibilities need to be revised based on the center's defined mission.

e. Develop standard processes and mechanisms to facilitate communication between the stakeholders and center personnel, to include in-person meetings and briefings on operational and administrative matters, as needed.

f. Develop and implement a Memorandum of Understanding (MOU) or Agreement (MOA) and, if needed, nondisclosure agreements (NDA) between the center and each stakeholder who intends to participate in or partner with the fusion center. (Review Guideline 5 for further details.)

g. Ensure that appropriate legal authorities review the agreements before signature.

h. Identify the organizations with executive and legislative oversight and funding responsibilities, and provide routine briefings on the establishment and operations of the center.

Recommended Resources

- *Refer to Appendix C: Functional Categories, Fusion Center Guidelines, for a list of organizations, disciplines, and functions to consider including as stakeholders.*
- *See Guidelines 4 and 5, Fusion Center Guidelines, for issues to consider when developing MOUs, MOAs, and NDAs.*

21 Those fusion centers utilizing an all-crimes approach that includes gang-related criminal intelligence are encouraged to consult Global's *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces* to assist in the coordination and/or implementation of their efforts.

4. **Policies and Procedures Manual—Fusion centers shall develop a policies and procedures manual for center operations. (Guideline 15, *Fusion Center Guidelines*)**

   a. Include the center's mission, goals, policies, procedures, rules, and regulations.

   b. Include the center's privacy policy and its physical and information security policies within the manual, which should include guidance on the use of information specifically for criminal investigations and compliance with local and state confidentiality laws and how to safeguard information.

   c. Outline the roles and responsibilities of all entities involved in the center and their function.

   d. Outline the day-to-day management and command structure of the center.

   e. Include in the manual the relevant processes developed in accordance with the Planning and Requirements Development capabilities (Section I.A.), to include outlining how and from whom intelligence requirements are developed.

   f. Implement an annual review of center directives, and purge or revise outdated policies and procedures.

5. **Center Performance—Fusion centers shall define expectations, measure performance, and determine effectiveness of their operations. (Guideline 16, *Fusion Center Guidelines*)**

   a. Develop outputs and outcomes that measure expected performance of identified mission, goals, and objectives.

   b. Coordinate the development and review of measures and performance with participating agencies.

   c. Create internal measures pertaining to administrative matters and external measures to evaluate the performance of the intelligence cycle. (See Section I.F., Reevaluation.)

   d. Utilize participation in a regular cycle of exercises to evaluate capabilities and assess performance. (See Section I.A.10.)

   e. To the extent possible, leverage systems and databases to statistically capture, store, and report performance.

   f. Publicize performance to the public, policymakers, and customers.

6. **Outreach—Fusion centers shall establish a policy to govern official outreach and communications with leaders and policymakers, the public sector, the private sector, the media, and citizens and develop a plan to enhance awareness of the fusion center's purpose, mission, and functions. (Guidelines 12 and 13, *Fusion Center Guidelines*)**

   a. Outreach efforts should include information about the center's privacy policy, the Fusion Process, and the types of information that should be reported to law enforcement or the fusion center and how to do so.

   b. If there is more than one fusion center operating within the state, the centers should jointly determine how to communicate the value, roles, and responsibilities of each of the centers, consistent with the plan required by Section I.A.1.

   c. Develop a process to liaise with and educate elected officials and community leadership to promote awareness of center operations.

   d. Train personnel on communications policy.

B. Information Privacy Protections[22]

"Develop, publish, and adhere to a privacy and civil liberties policy." – Guideline 8, Fusion Center Guidelines.

"Protecting the rights of Americans is a core facet of our information sharing efforts. While we must zealously protect our Nation from the real and continuing threat of terrorist attacks, we must just as zealously protect the information privacy rights and other legal rights of Americans. With proper planning we can have both enhanced privacy protections and increased information sharing – and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people." – National Strategy for Information Sharing, p. 27.

22 These capabilities were developed to ensure that the privacy policies that fusion centers develop are at least as comprehensive as the ISE Privacy Guidelines (see the Methodology section for further background). The achievement of these capabilities will result in a fusion center privacy protection policy that meets the Section 12.d. requirement of the ISE Privacy Guidelines.

1. **Privacy Official—Fusion centers shall designate an individual to serve as the privacy official and/or establish a privacy committee to be responsible for coordinating the development, implementation, maintenance, and oversight of the privacy protection policies and procedures. (ISE Privacy Guidelines—Section 12)**

   a. If the privacy official is not an attorney, the fusion center shall have access to legal counsel to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and assist with the development of policies, procedures, guidelines, and operation manuals.

   b. The privacy official or committee should review all other fusion center policies and procedures to ensure consistency with the privacy policy.

   c. The privacy official or committee shall coordinate with the center's designated security officer to ensure that security measures provide the proper protection to information in compliance with all applicable laws and the center's privacy policy protection policies.

   d. Identify stakeholders to include nongovernment organizations, advocates, the media, and others that are essential to the development and implementation of the privacy policy.

      i. To the extent possible, fusion centers should use existing outreach mechanisms, such as a state or local government's privacy advisory committee, or outreach conducted by the state or local law enforcement or homeland security organizations to facilitate engagement with the community and privacy advocacy groups.

2. **Privacy Policy Development—In developing the privacy policy, fusion centers shall:**

   a. Develop guidance statements that include the vision, mission, values statements, goals, and objectives for the creation of the privacy policy. (ISE Privacy Guidelines—Section 3)

   b. Develop a project charter that will include an introduction, background, membership, and the previously drafted guidance statements.

   c. Analyze the flow of information and the legal environment for the protection of privacy

to identify what gaps exist between existing technological and legal requirements.

i. Information flow analysis helps determine what personally identifiable information the agency collects, uses, maintains, and disseminates. (ISE Privacy Guidelines—Section 4)
   a) Identify the fusion center's data holdings and establish mechanisms to ensure their review before protected information is shared through the ISE.
   b) Establish mechanisms to identify the nature of protected information so it can be handled in accordance with applicable legal requirements.

ii. All policies and procedures are compliant with the U.S. Constitution, the state's constitution, applicable laws, and executive orders. (ISE Privacy Guidelines—Section 2)
   a) Conduct a rules assessment and adopt policies and procedures requiring the fusion center to seek, receive, or retain only the protected information which it is legally permitted to seek, receive, or retain and which was lawfully obtained.
   b) Establish a process to allow for the ongoing identification and assessment of new and/or revised laws, court decisions, and policies that impact issues related to privacy, civil rights, and civil liberties.
   c) If an issue posing a significant risk to privacy is identified, develop policy and procedural protections.

d. Perform a gap analysis to identify legal and technological gaps.

e. Vet the privacy protection policy internally and externally during its development by soliciting commentary and buy-in from stakeholders and agency constituents prior to finalizing the policy.

f. Formally adopt a privacy protection policy to guide the collection, use, maintenance, and dissemination of personal information. (ISE Privacy Guidelines—Section 12.d.)
   i. Obtain formal adoption of the policy by the project team, privacy and civil liberties officer, the fusion center's governance structure and, if applicable, any legislative body.

3. Privacy Protections—Fusion centers shall develop and implement a privacy protection policy that ensures that the center's activities (collection/gathering, analysis, dissemination, storage, and use of information) are conducted in a manner that protects the privacy, civil liberties, and other legal rights of individuals protected by applicable law, while ensuring the security of the information shared. The policy shall cover all center activities and shall be at least as comprehensive as the requirements set forth in the Information Sharing Environment Privacy Guidelines and consistent with 28 CFR Part 23 and DOJ's Global *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*.

a. The privacy protection policy shall include procedures to ensure data quality. (ISE Privacy Guidelines—Section 5)
   i. Establish accuracy procedures to ensure that information is accurate, and prevent, identify, and correct errors regarding (1) protected information and (2) any erroneous sharing of information in the ISE.
   ii. Establish and implement a process to provide written error notice of any potential error or deficiency to the privacy official of the source agency when it is determined that the protected information received may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected.
   iii. Adopt and implement the ISE policies and procedures for merger of information, investigation, and correction/deletion/nonuse of erroneous or deficient information, and retain only information that is relevant and timely for its appropriate use.

b. Establish criteria for types of information that partners can submit to the center.

c. Include provisions for the use of privately held data systems information and commercially obtained data.

d. Review the center's security policies and ensure that they are sufficient for providing appropriate physical, technical, and administrative measures to safeguard protected information. (See Section II.C. and ISE Privacy Guidelines—Section 6.)
   i. Ensure that the center's privacy and civil liberties policy articulates a process for responding to and addressing security breaches, in coordination with the center's designated security officer. (See Section II.C.2.)

e. The privacy protection policy shall include documentation on how the policies and procedures meet the following ISE Privacy Guidelines requirements (ISE Privacy Guidelines—Section 12):
   i. Fusion centers shall adopt policies and procedures limiting the sharing of information through the ISE to terrorism, homeland security, and law enforcement (terrorism-related) information, as defined for the ISE (see Glossary) and ensure that access to and use of protected information[23] are consistent with the authorized purpose of the ISE.[24] (ISE Privacy Guidelines—Section 3)
   ii. Fusion centers shall identify protected information to be shared through the ISE.

4. Privacy Policy Outreach—Fusion centers shall implement necessary outreach and training for the execution, training, and technology aspects of the privacy protection policy. (ISE Privacy Guidelines—Section 9)

a. Ensure that privacy protections are implemented through training, business process changes, and system designs.

b. Provide ongoing training to center personnel and any other liaison partners on the fusion center's privacy policies and procedures. Training should be tailored to the audience (management, analysts, collectors, consumers of center products, etc.) but, at a minimum, should include:
   i. An overview of the policies and procedures for collection, use, disclosure of protected information, data quality, accountability, enforcement, auditing, and redress.
   ii. How to report violations of the privacy policy.
   iii. An overview of sanctions or enforcement mechanisms for failure to comply with the privacy policy.

c. Consider and implement appropriate privacy-enhancing technologies.

d. Fusion centers shall facilitate public awareness of their privacy protection policy by making it available to the public or otherwise facilitating appropriate public awareness. (ISE Privacy Guidelines—Section 10)

5. Privacy Policy Accountability—Fusion centers shall ensure accountability with regard to the privacy protection policy and identify evaluation methods for auditing and monitoring the implementation of the privacy policy and processes to permit individual redress and incorporate revisions and updates identified through the evaluation and monitoring as well as redress processes. (ISE Privacy Guidelines—Section 7)

a. Fusion centers shall develop or modify policies, procedures, and mechanisms for accountability, enforcement, and auditing of the center's privacy protection. (ISE Privacy Guidelines—Section 7)
   i. Require reporting, investigating, and responding to violations of the center's privacy protection policy.
   ii. Encourage cooperation with audits and reviews.
   iii. Provide for receipt of error reports by the agency privacy official or committee. (See Section B.2., above.)
   iv. Implement adequate review and audit mechanisms to verify the center's compliance with its privacy protection policy.
   v. Incorporate the core elements of the ISE Privacy Guidelines' Accountability, Enforcement, and Audit guidance into the fusion center ISE privacy policy.

b. Fusion centers shall develop internal procedures for redress—particularly to address complaints from protected persons regarding personally identifiable information about them under fusion center control. (ISE Privacy Guidelines—Section 8)
   i. Incorporate the core elements of the ISE Privacy Guidelines Redress guidance into the fusion center ISE privacy protection policy.

23 The term "protected information" is defined in the ISE Privacy Guidelines, Section 1.b., for both non-intelligence agencies and members of the Intelligence Community. For both federal non-intelligence agencies and SLT agencies, it means, at a minimum, personally identifiable information about U.S. citizens and lawful permanent residents. States are free to extend this definition to other classes of persons or to all persons (including organizations).

24 The authorized purpose of the ISE is to share terrorism-related information in a lawful manner that protects the privacy and other legal rights of Americans between and among authorized recipients of such information. (ISE Privacy Guidelines—Section 3)

c. Fusion centers should utilize the LEIU *Audit Checklist for the Criminal Intelligence Function* when reviewing their "criminal intelligence function to demonstrate their commitment to protecting the constitutional rights and the privacy of individuals, while ensuring the operational effectiveness of their criminal intelligence function."[25]

C. Security

"Ensure appropriate security measures are in place for the facility, data, and personnel." – Guideline 9, Fusion Center Guidelines.

1. Security Measures—Fusion centers shall establish appropriate security measures, policies, and procedures for the center's facility (physical security), information, systems, and personnel and visitors and document them in a security plan consistent with the NCISP, the *Fusion Center Guidelines*, Global's *Applying Security Practices to Justice Information Sharing* document, and 28 CFR Part 23. (Guidelines 8, 9, and 10, *Fusion Center Guidelines*)

25 LEIU *Audit Checklist for the Criminal Intelligence Function*, p. i.

2. Security Officer—Fusion centers shall designate an individual to serve as the security officer responsible for coordinating the development, implementation, maintenance, and oversight of the security plan. (Guideline 9, *Fusion Center Guidelines*)

a. For fusion centers colocated with other organizations (e.g., HIDTA, FBI), the fusion center can opt to use the other organization's security officer, provided that the officer is willing to perform the capabilities required of the fusion center security officer. If a colocated organization's security officer cannot or will not perform all of the functions, the fusion center should designate an individual to partner with the other organization's security officer to ensure that each of the baseline capabilities for security is met.

b. Ensure that the designated security officer has at least some exposure to or experience with physical, information, systems, and/or personnel security.

c. Ensure that the security officer receives routine training in the areas of physical, information, systems, and personnel security, to include the relevant DHS- or FBI-required training if the fusion center intends to establish and maintain a certified storage environment at the Secret level.

d. The security officer should:

i. Conduct security training and awareness on the center's overall security plan and the center's security measures, policies, and procedures.

ii. Provide regular updates to the center's management and the governance body on compliance with the security plan.

iii. Coordinate with federal security officials to the extent needed for facilitating federal security clearances for personnel, facility security certifications, and access to federal information systems. (Reference Section II.E. regarding security clearances for personnel.)

iv. Establish and coordinate the processes used to conduct background checks on all center personnel prior to commencement of duties. (Reference Section II.D.2.)

v. Receive, document, and investigate reports of security violations according to the center's security policies.

3. Securing Information—Fusion centers' security policies shall address the ability to collect, store, and share classified, controlled unclassified, and unclassified information to address homeland security and criminal investigations. (Guidelines 7 and 14, *Fusion Center Guidelines*)

a. In coordination with the appropriate federal security official, develop a process to receive, handle, store, and disseminate Secret-level information, to include establishing and maintaining a certified storage environment[26] if one is not readily available.[27]

b. Fusion centers shall follow the regulations and processes for security management of the certified storage environment, as required by the federal security manager (i.e., DHS or FBI), to include, but not limited to:

i. Certification of computers and other electronic devices for classified information.

ii. Storage of both paper and electronic media containing classified information.

iii. Level of security clearance required to access the facility without escort.

iv. Processes for certifying the security clearances of individuals assigned to or visiting the facility.

v. Rules for access with escort for individuals not holding the requisite level of security clearance.

vi. Processes for derivative classification and marking of classified information created within the facility.

vii. Processes for dealing with any security incidents or violations that may take place.

c. In coordination with the appropriate federal agencies, establish a policy to receive, handle, store, and disseminate federal information that is provided under the Controlled Unclassified Information Framework. (See Glossary.)

26 Certified storage environments will either be DHS-certified Open Storage Secret or the equivalent FBI-certified closed storage environment. NOTE: The Open Storage authorization granted by DHS applies only to computer systems and not to document storage.

27 DHS and the FBI have agreed to allocate the responsibilities for the following support to fusion centers to minimize redundancy: establishing operating classified work environments, getting personnel cleared to be able to access classified information, providing ways to communicate with the federal government, and other technical assistance. See the most recent version of the Federal Coordinated Support Plan for further information regarding these efforts.

d. Ensure that security policies allow for timely distribution of the center's intelligence products to the center's constituency base, which may include daily, weekly, and monthly analysis reports and assessments; advisories; alerts; warnings; executive reports; briefings; etc.

e. If a fusion center has chosen to incorporate the CIKR discipline, it shall have the ability to collect, store, and share Chemical-terrorism Vulnerability Information (CVI) (in accordance with 6 CFR Part 27), Safeguards Information (SGI), Sensitive Security Information (SSI) (in accordance with 49 CFR Part 1520), and Protected Critical Infrastructure Information (PCII) in accordance with the PCII Final Rule.

f. Consider whether a state law for security and confidentiality of public and private sector data is needed.

g. Adopt established, accredited models for secure horizontal and vertical information and intelligence sharing (e.g., RISS, LEO, HSIN, OneDOJ).

h. Ensure that controls and safeguards for data access to all appropriate systems are in place.

D. Personnel and Training

"Achieve a diversified representation of personnel based on the needs and functions of the center." – Guideline 11, Fusion Center Guidelines.

1. Staffing Plan—Fusion center managers should develop a staffing plan based on the center's mission and goals and update as needed based on the current

information requirements, collection strategy, and analytic production plan. (Guideline 11, *Fusion Center Guidelines*)

a. Managers should determine which positions require access to classified national security information based on the roles and responsibilities of the position and, through the center's security officer, make the request for national security clearances to the federal security manager.[28]

b. Where appropriate, make clear when employment is contingent upon the applicant's ability to meet the requirements necessary for receiving national security clearances.

c. Adhere to the education and hiring standards for analysts in IALEIA and Global's *Law Enforcement Analytic Standards* booklet.[29]

d. The staffing plan should address the following support of functions: administration, information technology, communications, graphics, designated security officer (Section II.C.), and designated privacy official (Section II.B.).

e. The staffing plan should address the center's requirements to access legal counsel to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and liaison with the development of policies, procedures, guidelines, and operation manuals. (Also required by Section II.B.2.a.)

2. Background Checks—Ensure that background checks are conducted on center personnel (whether private or public) prior to the commencement of duties. (NCISP Recommendation 27 and Guideline 9, *Fusion Center Guidelines*)

3. Training Plan—Fusion centers shall develop and document a training plan to ensure that personnel and partners understand the intelligence process and the 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*)

a. Reference each capability grouping for further details on minimum training requirements for particular capabilities (e.g., Analysis and Production, Management and Governance, Information Privacy Protections, and Security).

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

   i. The intelligence process and types of intelligence, crime-specific training, and how these factors contribute to implementation of the center's collection plan, through the use of the NCISP training objectives and the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*.

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

   iii. The center's privacy and security policies and protocols.

c. Training should be provided to all fusion center personnel upon assignment to the center and include regular retraining.

   i. All fusion center personnel—including analysts, intelligence officers, and non-law enforcement personnel assigned to the center (corrections, fire services, public health, private sector, and others)—assigned both full-time, part-time, and on an "as needed" basis should be included in the training plan.

d. See Guidelines 12 and 13, *Fusion Center Guidelines*, for additional information.

28 See Footnote 21.

29 IALEIA and Global's *Law Enforcement Analytic Standards* booklet is available at http://www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf.

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

"Integrate technology, systems, and people."

– Guideline 10, Fusion Center Guidelines.

1. Business Processes Relating to Information Technology—Fusion centers shall identify and define their business processes prior to purchasing or developing information technology, communications infrastructure, systems, or equipment to handle those processes.

a. Utilize the methodology and templates for analyzing the fusion center's business architecture provided by the Global document *Fusion Center Business Architecture*.

2. Information Exchange within the Center—Fusion centers shall establish an environment in which center personnel and partners can seamlessly communicate—effectively and efficiently exchanging information in a manner consistent with the business processes and policies of the fusion center. (Guidelines 6, 7, and 10, *Fusion Center Guidelines*)

a. Ensure that appropriate personnel are colocated and/or virtually integrated within the center.

b. Leverage databases, systems, and networks available from participating entities to maximize information sharing, and plan for future connectivity to other federal, state, local, and tribal systems under development.

c. Utilize the latest version of NIEM for information exchange.

d. Maintain a repository of information to be made available to the Information Sharing Environment, which will be a component of ISE Shared Spaces.[30]

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.

c. Ensure that redundancy is incorporated into the plan.

d. Test the communications plan on a routine basis to ensure operability and maintenance of current contact information for fusion center participants.

e. See Guideline 18 for recommended aspects of the communications plan.

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*)

30 See Footnote 14 or the Glossary for more information on the ISE Shared Spaces concept.

a. Conduct a threat/vulnerability assessment to determine risk to the facility, data, and personnel.

b. Develop the plans in coordination with emergency managers and other appropriate response and recovery officials. (See Section I.A.8.)

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

d. Ensure that contact information for the constituency is up to date.

e. Ensure redundancy of infrastructure, resources, personnel, communications, and systems.

f. Establish an emergency power source.

g. Conduct continuity-of-operations exercises to ensure the operational resiliency of the center.

h. Reference Guidelines 9, 10, and 18 for recommended aspects for developing contingency and continuity-of-operations plans.

F. Funding

"Establish and maintain the center based on funding availability and sustainability."
– Guideline 17, Fusion Center Guidelines.

1. Investment Strategy – Fusion centers shall develop an investment strategy to achieve and sustain baseline capabilities for the center's operations, including a delineation of current and recommended future federal versus nonfederal costs. (Guideline 17, *Fusion Center Guidelines*)

a. Base funding on center priorities identified by center leadership.

b. Identify capability gaps and develop an investment strategy and resource plan to achieve the baseline capabilities.

c. Establish an operational budget.

d. Leverage existing resources/funding from participating entities and identify supplemental funding sources.

e. Ensure that resource commitment of participating entities is addressed in the MOU.

f. Identify return on investment for fusion center partners.

g. Engage executive and legislative officials who have oversight and funding responsibilities, and provide routine briefings on the establishment, operations, and budgetary needs of the center.

h. Ensure that the investment strategy is communicated to and coordinated with the state homeland security advisor (HSA) and State Administrative Agency (SAA) to ensure coordination and support of the state's homeland security strategy and any respective state and/or urban area grant program investment justifications.

Appendix A – Focus Group Participants

Mr. John D. Cohen
Advisor to the Program Manager
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National Intelligence

Major Daniel Cooney
Criminal Intelligence Section
New York State Intelligence Center
New York State Police

Mr. James Fullington
Special Agent in Charge
Georgia Information Sharing and
Analysis Center
Georgia Bureau of Investigation

Mr. Van Godsey
Director
Missouri Information Analysis Center
Missouri State Highway Patrol

Captain William T. Harris
Criminal Intelligence
Delaware Information Analysis Center
Delaware State Police

Captain Richard W. Holland
Criminal Intelligence Division
Houston, Texas, Police Department

Sergeant Lance Ladines
Washington Joint Analytical Center
Washington State Patrol

Mr. Don R. Ladner, Jr.
Assistant Special Agent in Charge
Office of Statewide Intelligence
Florida Department of Law Enforcement

Mr. J. Patrick McCreary
Associate Deputy Director
Policy Office
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Mr. Michael Mines
Deputy Assistant Director
Directorate of Intelligence
Federal Bureau of Investigation

Mr. Thomas J. O'Reilly
Senior Policy Advisor for Information Sharing
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Mr. Tim Parry
Senior Investigator
Counter Terrorism Center
New York State Intelligence Center
New York State Police

Captain Charles Rapp
Maryland Coordination and Analysis Center
Baltimore County Police Department

Mr. Robert C. Riegle
Director, State and Local Program Office
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Mr. Kevin Saupp
Section Chief, Prevention and Protection
National Preparedness Directorate
U.S. Department of Homeland Security

Appendix B – Baseline Capabilities Crosswalk

Each Baseline Capability is listed, followed by bullets indicating the sections of the documents related to that capability.

- TCL refers to the *Target Capabilities List*, September 2007.
- NCISP refers to the *National Criminal Intelligence Sharing Plan*.
- FCG refers to the *Fusion Center Guidelines*.
- NSIS refers to the *National Strategy for Information Sharing*.

I. Fusion Process Capabilities

A. Planning and Requirements Development

1. Intrastate Coordination—In developing and implementing all Fusion Process-related plans and procedures, the center shall coordinate with other fusion centers (the designated state fusion center and/or any UASI fusion center(s)) within its state to identify the roles and responsibilities of each center in carrying out the Fusion Process (gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information) on a statewide basis.
   - TCL ComG 1.1.1
   - TCL ComG 1.4.2
   - TCL ComG 3.1
   - TCL ComG 4.1
   - TCL ComG 5.1
   - TCL Pre.A1b 1.3
   - TCL Pre.A1b 1.5
   - TCL Pre.A1c 3.1
   - TCL PreC1a 1.1
   - FCG Guideline 4
   - NSIS, Appendix 1, II. SLT Responsibility 5
2. Risk Assessment—Fusion centers shall conduct or contribute to a statewide and/or regional risk assessment that identifies and prioritizes threats, vulnerabilities, and consequences at regular intervals.
   - FCG Guideline 14
   - NSIS, Appendix 1, III. SLT Responsibility 1
3. Information Requirements—The information requirements for the fusion center shall be defined, documented, updated regularly, and consistent with the center's goals and objectives as defined by the governance structure and reflect the risks identified in the statewide and/or regional risk assessment.
   - TCL Pre.A1b 1.3
   - TCL Pre.A1b 1.4
4. Suspicious Activity Reporting (SAR)—Fusion centers shall develop, implement, and maintain a plan to support the establishment of a suspicious activity and incident reporting process for their geographic area of responsibility, in a manner consistent with the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*.[31] Specifically, centers shall have the ability to receive, process, document, analyze, and share SARs in a manner that complies with the ISE-SAR Functional Standard.
   - TCL Pre.A1b 4.1
   - TCL Pre.A1b 4.2
   - TCL Pre.A1b 4.3
   - TCL Pre.A1b 4.4
   - NSIS, Appendix 1, III. SLT Responsibilities
5. Alerts, Warnings, and Notifications—Fusion centers shall ensure that alerts, warnings, and notifications are disseminated, as appropriate, to state, local, and tribal authorities; the private sector; and the general public.
   - TCL Pre.A1b 1.5

31 The Major Cities Chiefs Association, Global, DOJ, and DHS supported the development of this report, which describes "the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity by the local police agency."

- TCL Pre.A1b 1.7
- NSIS, Appendix 1, IV. SL Responsibilities

6. Situational Awareness Reporting—Fusion centers shall develop processes to manage the reporting to key officials and the public of information regarding significant events (local, regional, national, and international) that may influence state or local security conditions.
   - NSIS, Appendix 1, V. SL Responsibilities
7. Data Sources—Fusion centers shall identify and document data sources and repositories needed to conduct analysis based on the mission of the center, the findings of the Risk Assessment, and the center's defined Information Requirements.
   - TCL Pre.A1b 5.2
   - TCL Pre.A1c 3.2.1
   - FCG Guideline 6
8. Coordination With Response and Recovery Officials—Fusion centers shall identify and coordinate with emergency managers and appropriate response and recovery personnel and operations centers to develop, implement, and maintain a plan and procedures to ensure a common understanding of roles and responsibilities and to ensure that intelligence and analysis capabilities can be leveraged to support emergency management operation activities, as appropriate, when events require such a response.
   - TCL ComG 5.1.1
   - TCL Pre.C1a 3.5.2
9. Coordination With Private Sector and Critical Infrastructure and Key Resources (CIKR) Information Sharing—Fusion centers, in partnership with locally based federal authorities, shall develop, implement, and maintain a plan and procedures for sharing information with owners of CIKR and, in general, the private sector, in a coordinated manner.
   - TCL ComG 5.2
   - TCL Pre.C1a 3.6
   - TCL Pre.C1a 3.2.1.2
   - FCG Guideline 3
   - NCISP Recommendation 7
10. Exercises—Fusion centers should conduct or participate in another agency's scenario-based tabletop and live training exercises to regularly assess their capabilities.
    - TCL ComG 2.2.1
    - TCL Pre.C1a 2.2.2
    - FCG Guideline 12

B. Information Gathering/Collection

1. Information-Gathering and -Reporting Strategy—Fusion centers shall develop, implement, and maintain an information-gathering and -reporting strategy that leverages existing capabilities and shall identify methods for communicating information requirements and the overall information-gathering strategy to partners, to include any applicable fusion liaison officers.
   - TCL Pre.A1b 3.1
   - TCL Pre.A1b 3.1.1
   - TCL Pre.A1b 3.2
   - TCL Pre.A1b 3.3
   - TCL Pre.A1b 3.3.1
   - TCL Pre.A1b 5.3
   - TCL Pre.A1c 4.1
2. Feedback Mechanism—Fusion centers shall define and implement a feedback mechanism that:
   a. Provides the reporting entity an acknowledgement of the receipt of its information and, to the extent possible, provides feedback on the value of the information and actions taken with the information.
   b. Allows collectors to make suggestions to improve the strategy, plans, or processes, as well as seek clarification on information requirements.
   c. Allows recipients of information or products to make suggestions to improve products.
      - TCL Pre.A1b 1.4
      - TCL Pre.A1b 1.6
3. Collection and Storage of Information—Fusion centers shall define the policies and processes and establish a mechanism for receiving, cataloging, and retaining information provided to the center.
   - TCL Pre.A1b 1.2
   - TCL Pre.A1b 3.1.2
   - TCL Pre.A1c 6.3
   - FCG Guideline 6
   - NCISP Recommendations 9 and 11

C. Processing and Collation of Information

1. Information Collation—Fusion center analysts shall use the necessary and available tools to process and collate information and intelligence to assist with accurate and timely analysis.
   - TCL Pre.A1b 3.1.2
   - TCL Pre.A1b 5.3
   - TCL Pre.A1b 1.2
   - TCL Pre.A1c 5.1
   - TCL Pre.A1c 5.2.1
2. Levels of Confidence—Fusion centers shall liaise with partners to ensure that information collected is relevant, valid, and reliable.
   - TCL Pre.A1c 4.2

D. Intelligence Analysis and Production

1. Analytic Products—Fusion centers shall develop, implement, and maintain a production plan that describes the types of analysis and products they intend to provide for their customers and partners (which, at a minimum, include Risk Assessments; Suspicious Activity Reporting; Alerts, Warnings, and Notifications; and Situational Awareness Reporting [see Sections I.A.2, 4, 5, and 6 for further details on these product types]), how often or in what circumstances the product will be produced, and how each product type will be disseminated.
   - TCL Pre.A1c 1.1.3
   - TCL Pre.A1c 1.2
   - TCL Pre.A1c 1.3.2
   - TCL Pre.A1c 6.2
   - FCG Guideline 14
2. Fusion Process Management—An intelligence commander/manager should be designated to oversee the management of the Fusion Process (including the collection, collation, analytic function, dissemination, and reevaluation of information and intelligence) within the center.
3. Enhancing Analyst Skills—The fusion center should develop and implement a Training and Professional Development Plan to enhance analysts' critical thinking, research, writing, presentation, and reporting skills.
   - TCL Pre.A1c 1.4.1
   - FCG Guideline 12
4. Information Linking—Fusion centers shall ensure that analysts are able to understand and identify the links between terrorism-related intelligence and information related to traditional criminal activity so they can identify activities that are indicative of precursor behaviors, terrorist activities, and threats.
   - TCL Pre.A1c 5.2.3
   - TCL Pre.C1a 3.5
   - TCL Pre.C1a 3.5.1
   - FCG Guidelines 12, 13, and 14
5. Strategic Analysis Services—Fusion centers shall develop the capability to provide strategic analysis services for the jurisdiction served.
   - TCL Pre.A1c 5.2.2
   - FCG Guideline 14
6. Open Source Analysis Capability—Fusion centers shall establish an open source analysis capability utilizing the free training and tools provided by the federal government.
7. Analyst Specialization—Fusion centers should assign "accounts" or "specialties" to analysts based on the priorities of the fusion center, to allow the development of analytic depth.
   - FCG Guideline 11
8. Analytical Tools—Fusion centers shall provide the necessary tools to analysts for the analysis of information and data.
   - TCL Pre.A1c 5.2.4
   - FCG Guidelines 11 and 14
   - NCISP Recommendation 28

E. Intelligence/Information Dissemination

1. Dissemination Plan—Fusion centers shall develop a high-level dissemination plan that documents the procedures and communication mechanisms for the timely dissemination of the center's various products to the core and ad hoc customers.
   - TCL ComG 3.1
   - TCL ComG 3.1.1
   - TCL ComG 4.1.2
   - TCL Pre.A1c 1.3
   - TCL Pre.A1c 6.1
   - TCL Pre.C1a 4.4
2. Reporting of Information to Other Centers—Fusion centers shall develop the processes and protocols for ensuring that relevant and vetted priority information is reported to fusion centers in other states and localities to support regional trends analysis.
   - TCL ComG 3.1
   - TCL ComG 4.1.1
   - TCL Pre.A1c 1.3.1
   - TCL Pre.A1c 3.3
   - TCL Pre.C1a 1.1
   - TCL Pre.A1c 6.4
   - FCG Guidelines 7 and 14
3. Reporting of Information to Federal Partners—Fusion centers shall develop the processes and protocols, in coordination with the FBI and DHS Office of Intelligence and Analysis (I&A), for ensuring that relevant and vetted priority information is reported to the JTTF and other appropriate federal agencies to support its inclusion into national patterns and trends analysis.
   - TCL ComG 3.1
   - TCL ComG 4.1.1
   - TCL Pre.A1b 1.4
   - TCL Pre.A1c 3.4
   - TCL Pre.C1a 4.1
   - TCL Pre.C1a 4.1.1

F. Reevaluation

1. Performance Evaluation—Fusion centers shall develop and implement a plan to reevaluate the center's performance of the intelligence cycle on a regular basis.
   - FCG Guideline 16

2. Fusion Center Processes Review—Fusion centers shall establish a process to review and, as appropriate, update the center's information requirements, collection plan, and analytic production strategy on a regular basis and any time one of the following is received:

   a. New threat or vulnerability information;

   b. New federal or state standing or ad hoc information requirements;

   c. Federal or state alerts, warnings, or notifications or situational awareness bulletins; and/or

   d. Updated risk assessment.
      - FCG Guideline 16

II. Management and Administrative Capabilities

A. Management/Governance

1. Governance Structure—Fusion centers shall have a governance structure that provides appropriate representation for the jurisdictions and disciplines in the center's area of responsibility.
   - FCG Guidelines 3, 4, and 5

2. Mission Statement—Fusion centers shall have a defined mission statement that is clear and concise and conveys the purpose, priority, and roles of the center.
   - FCG Guideline 2

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.
   - TCL ComG 1.1.1
   - TCL ComG 1.1.2
   - FCG Guidelines 4, 5, and 11

4. Policies and Procedures Manual—Fusion centers shall develop a policies and procedures manual for center operations.
   - TCL ComG 1.3
   - TCL Pre.A1b 1.1
   - FCG Guideline 15

5. Center Performance—Fusion centers shall define expectations, measure performance, and determine effectiveness of their operations.
   - FCG Guideline 16

6. Outreach—Fusion centers shall establish a policy to govern official outreach and communications with leaders and policymakers, the public sector, the private sector, the media, and citizens, and develop a plan to enhance awareness of the fusion center's purpose, mission, and functions.
   - TCL Pre.C1a 4.2
   - FCG Guidelines 12 and 13

B. Information Privacy Protections

1. Privacy Official—Fusion centers shall designate an individual to serve as the privacy official and/or establish a privacy committee to be responsible for coordinating the development, implementation, maintenance, and oversight of the privacy protection policies and procedures.
   - FCG Guideline 8
   - ISE Privacy Guidelines—Section 12

2. Privacy Policy Development—In developing the privacy policy, fusion centers shall:

   a. Develop guidance statements that include the vision, mission, values statements, goals, and objectives for the creation of the privacy policy.

   b. Develop a project charter that will include an introduction, background, membership, and the previously drafted guidance statements.

   c. Analyze the flow of information and the legal environment for the protection of privacy to identify what gaps exist between existing technological and legal requirements.

   d. Vet the privacy protection policy internally and externally during its development by soliciting commentary and buy-in from stakeholders and agency constituents prior to finalizing the policy.

   e. Formally adopt a privacy protection policy to guide the collection, use, maintenance, and dissemination of personal information.
      - TCL ComG 1.4
      - FCG Guideline 8
      - ISE Privacy Guidelines—Section 12.d.
      - ISE Privacy Guidelines—Section 3
      - NCISP Recommendation 6

3. Privacy Protections—Fusion centers shall develop and implement a privacy protection policy that ensures that the center's activities (collection/gathering, analysis, dissemination, storage, and use of information) are conducted in a manner that protects the privacy, civil liberties, and other legal rights of individuals protected by applicable law, while ensuring the security of the information shared. The policy shall cover all center activities and shall be at least as comprehensive as the requirements set forth in the Information Sharing Environment Privacy Guidelines and consistent with 28 CFR Part 23 and DOJ's Global *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*.
   - TCL ComG 1.2.1
   - TCL ComG 3.1.2
   - TCL Pre.A1c 3.6
   - FCG Guideline 8
   - NCISP Recommendations 9 and 15

4. Privacy Policy Outreach—Fusion centers shall implement necessary outreach and training for the execution, training, and technology aspects of the privacy protection policy.
   - FCG Guideline 8
   - ISE Privacy Guidelines—Section 9

5. Privacy Policy Accountability—Fusion centers shall ensure accountability with regard to the privacy protection policy and identify evaluation methods for auditing and monitoring the implementation of the privacy policy and processes to permit individual redress and incorporate revisions and updates identified through the evaluation and monitoring as well as redress processes.
   - TCL ComG 3.1.3
   - FCG Guideline 8
   - ISE Privacy Guidelines—Section 7

C. Security

1. Security Measures—Fusion centers shall establish appropriate security measures, policies, and procedures for the center's facility (physical security), information, systems, and personnel and visitors and document them in a security plan consistent with the NCISP, the *Fusion Center Guidelines*, Global's *Applying Security Practices to Justice Information Sharing* document, and 28 CFR Part 23.
   - TCL Pre.A1c 3.6
   - FCG Guidelines 8, 9, and 10

2. Security Officer—Fusion centers shall designate an individual to serve as the security officer responsible for coordinating the development, implementation, maintenance, and oversight of the security plan.
   - FCG Guideline 9

3. Securing Information—Fusion centers' security policies shall address the ability to collect, store, and share classified, controlled unclassified, and unclassified information to address homeland security and criminal investigations.
   - TCL ComG 3.1.2
   - FCG Guidelines 7 and 14

D. Personnel and Training

1. Staffing plan—Fusion center managers should develop a staffing plan based on the center's mission and goals and update as needed based on the current information requirements, collection strategy, and analytic production plan.
   - TCL Pre.A1c 1.4
   - FCG Guideline 11

2. Background Checks—Ensure that background checks are conducted on center personnel (whether private or public) prior to the commencement of duties.
   - TCL Pre.C1a 1.7
   - NCISP Recommendation 27
   - FCG Guideline 9

3. Training Plan—Fusion centers shall develop and document a training plan to ensure that personnel and partners understand the intelligence process and the 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.
   - TCL ComG 2.1.1
   - TCL Pre.A1b 2.1.1
   - TCL Pre.A1c 2.1.1
   - TCL Pre.A1c 1.4.1
   - TCL Pre.C1a 1.3
   - TCL Pre.C1a 2.1.3
   - FCG Guidelines 12 and 13
   - NCISP Recommendation 18

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

1. Business Processes Relating to Information Technology—Fusion centers shall identify and define their business processes prior to purchasing or developing information technology, communications infrastructure, systems, or equipment to handle those processes.
   - FCG Guideline 7

2. Information Exchange Within the Center—Fusion centers shall establish an environment in which center personnel and partners can seamlessly communicate—effectively and efficiently exchanging information in a manner consistent with the business processes and policies of the fusion center.
   - TCL ComG 1.2.1
   - TCL Pre.A1b 5.1
   - TCL Pre.A1c 3.2.1
   - FCG Guidelines 6, 7, and 10

3. Communications Plan—Fusion centers shall have a plan to ensure safe, secure, and reliable communications, including policies and audit capabilities.
   - TCL Pre.A1c 3.3
   - FCG Guideline 18
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.
   - TCL ComG 1.2.2
   - TCL ComG 1.4.3
   - TCL Pre.A1c 3.2.2
   - FCG Guidelines 9, 10, and 18

F. Funding

1. Investment Strategy—Fusion centers shall develop an investment strategy to achieve and sustain baseline capabilities for the center's operations, including a delineation of current and recommended future federal versus nonfederal costs.
   - FCG Guideline 17
   - NSIS Appendix 1, II. SLT Responsibility 4

Appendix C—Glossary of Terms

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:

Right to Know
Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

Need to Know
As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation.

Investigatory Value
Intelligence or information is disseminated in the law enforcement community for surveillance, apprehension, or furtherance of an investigation.

Public Value
Intelligence or information can be released to the public when there is a need to know and a right to know the information because of the value that may be derived from public dissemination, to (1) aid in locating targets/suspects and (2) for public safety purposes (i.e., hardening targets, taking precautions).

Administrative Analysis
The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions.

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 its 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
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.

Allocation
Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

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.

Archiving (Records)
The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

Association Analysis
The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix.

Automated Trusted Information Exchange™ (ATIX)
Operated by the Regional Information Sharing Systems, ATIX is a secure means to disseminate national security or terrorist threat information to law enforcement and other first responders via the ATIX electronic bulletin board, secure Web site, and secure e-mail.

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.

Bias/Hate Crime
Any criminal act directed toward any person or group as a result of that person's race, ethnicity, religious affiliation, or sexual preference.

Capabilities-Based Preparedness
"Preparing, under uncertainty, to provide capabilities suitable for a wide range of challenges while working within an economic framework that necessitates prioritization and choice." (Source: *National Preparedness Guidelines,* p. 30.)

Clandestine Activity
An activity that is usually extensive and goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. "Storefront" operations, "stings," and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine collections.

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.

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

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

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

Collation (of information)
A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

Collection (of information)
The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

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

Commodity (Illegal)
Any item or substance that is inherently unlawful to possess (contraband) or materials which, if not contraband, are

themselves being distributed, transacted, or marketed in an unlawful manner.

Commodity Flow Analysis
Graphic depictions and descriptions of transactions, shipment, and distribution of contraband goods and money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities.

Common Terrorism Information Sharing Standards (CTISS)
Business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: functional standards and technical standards. Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas. Technical standards document specific technical methodologies and practices to design and implement information sharing capability into ISE systems. CTISS, such as ISE-SAR, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the *ISE Enterprise Architecture Framework*.

Conclusion
A definitive statement about a suspect, action, or state of nature based on the analysis of information.

Confidential
See Classified Information/Intelligence, Confidential Classification.

Continuing Criminal Enterprise
Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity, that are involved in a continuing or perpetuating criminal activity.

Controlled Unclassified Information (CUI)
"A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU)." (Presidential Memorandum to Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information [CUI], May 7, 2008.)

Controlled Unclassified Information (CUI) Framework and Implementation
Refers to the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of CUI terrorism-related information that originates in departments and agencies, regardless of the medium used for the display, storage, or transmittal of such information. The President's May 7, 2008, Memorandum directed all federal agencies to implement the CUI Framework, which consists of policies and standards for the designation, marking, safeguarding, and dissemination of any CUI terrorism-related information within the ISE that originates in federal agencies, regardless of the medium used for its display, storage, or transmittal. The President designated the National Archives and Records Administration (NARA) as the Executive Agent responsible for overseeing and managing implementation of the framework, to include the development of CUI policy standards and implementation guidance. Implementation is expected to occur over a 5-year transition period. The Memorandum designates that all CUI shall merit one of two levels of safeguarding procedures—standard (marked "Controlled") or enhanced (marked "Controlled Enhanced")—and one of two levels of dissemination controls—"Standard Dissemination" or "Specified Dissemination." This allows for three combinations of safeguarding procedures and dissemination controls:

(i) **"Controlled with Standard Dissemination"**—meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

(ii) **"Controlled with Specified Dissemination"**—meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

(iii) **"Controlled Enhanced with Specified Dissemination"**—meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

With regards to the CUI Framework's application to state, local, tribal, and private sector entities:

- The CUI Memorandum applies only to federal Executive Branch departments and agencies that handle and share terrorism-related information or are participants in the Information Sharing Environment.

- State and local government officials participated extensively in developing the framework, and many have indicated that they will voluntarily adopt the CUI Framework.

- The President directed NARA to develop and issue CUI policy standards and implementation guidance consistent with the Memorandum, to include appropriate recommendations for state, local, tribal, private sector, and foreign partner entities for implementing the CUI Framework.

- The Memorandum directs that federal agencies receiving CUI which originated from a state, local, tribal, private sector, or foreign partner shall retain any nonfederal legacy markings, unless the originator authorizes its removal.

- The Information Sharing Council's State, Local, Tribal, and Private Sector Subcommittee will be consulted during the development of procedures, guidelines, and standards necessary to establish, implement, and maintain the CUI Framework.

(Presidential Memorandum to Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information [CUI], May 7, 2008.)

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

Counterintelligence
"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." One type of intelligence included in the "National Intelligence" or "Intelligence Related to National Security" definitions. (50 U.S.C. § 401a; Section 3 of the National Security Act of 1947, as amended.)

Covert Intelligence
A covert activity planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity.

Crime Analysis
The process of analyzing information collected on crimes and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

Crime-Pattern Analysis
An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables.

Criminal History Record Information (CHRI)
Information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any disposition arising therefrom, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Criminal Informant
See Informant.

Criminal Intelligence
See Intelligence (Criminal) and Law Enforcement Intelligence.

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

Criminal Predicate
Information about an individual or his/her behavior that may only be collected and stored in a law enforcement intelligence records system when there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

Data Element
A field within a database that describes or defines a specific characteristic or attribute.

Data Owner
The agency that originally enters information or data into a law enforcement records system.

Data Quality
Controls implemented to ensure that all information in a law enforcement agency's records system is complete, accurate, and secure.

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

Deductive Logic
The reasoning process of taking information and arriving at conclusions from within that information.

Deployment
The short-term assignment of personnel to address specific crime problems or police service demands.

Designated State and/or Major Urban Area Fusion Center
The fusion center in each state designated as the primary or lead fusion center for the information sharing environment.

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.

Due Process
Fundamental fairness during the course of the criminal justice process, including adherence to legal standards and the civil rights of the police constituency; the adherence to principles that are fundamental to justice.

El Paso Intelligence Center (EPIC)
A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Its primary concern is drug trafficking; however, intelligence on other crimes is also managed by EPIC.

Enterprise
Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity.

Estimate
See Intelligence Estimate.

Evaluation (of Information)
Review of all information collected for the intelligence cycle for its quality, with an assessment of the validity and reliability of the information.

Event Flow Analysis
Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event, intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events.

Exemptions (to the Freedom of Information Act)
Circumstances wherein a law enforcement agency is not required to disclose information from a Freedom of Information Act (FOIA) request.

Field Intelligence Group (FIG)
The centralized intelligence component in a Federal Bureau of Investigation (FBI) field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

Field Intelligence Report (FIR)
An officer-initiated interview of a person believed by the officer to be acting in a suspicious manner that may be indicative of planning or preparing to conduct criminal activity.

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

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

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

Forecast (as related to Criminal Intelligence)
The product of an analytic process that provides a probability of future crimes and crime patterns based upon a comprehensive, integrated analysis of past, current, and developing trends.

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

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. Federal agencies will provide terrorism-related information to state, local, and tribal authorities primarily through these fusion centers, which may further customize such information for dissemination to satisfy intra- or interstate needs. Likewise, fusion centers enable the effective communication of locally generated terrorism-related information to the federal government and other fusion centers through the ISE. (*National Strategy for Information Sharing*, October 2007.)

***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. The guidelines were developed by law enforcement intelligence, public safety, and private sector subject-matter experts through the Global Justice Information Sharing Initiative and the Homeland Security Advisory Council. The Guidelines have been endorsed by the U.S. Departments of Justice and Homeland Security and the *National Strategy for Information Sharing*.

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.)

Guidelines
See Intelligence Records Guidelines.

Homeland Security Advisory System
An information and communications structure designed by the U.S. government for disseminating information to all levels of government and the American people regarding the risk of terrorist attacks and for providing a framework to assess the risk at five levels: Low, Guarded, Elevated, High, and Severe.

Hypothesis (from Criminal Intelligence Analysis)
An interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proven or disproved by further investigation and analysis.

Indicator
Generally defined and observable actions that, based on an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act.

Inductive Logic
The reasoning process of taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

Inference Development
The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based upon the use of inductive or deductive logic in the analysis of raw information related to the target.

Informant
An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself/herself from prosecution and/or provide the information in exchange for payment.

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 Evaluation
See Evaluation (of Information).

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.

ISE Shared Spaces Concept or Shared Spaces
The ISE Shared Spaces concept is a key element of the *ISE Enterprise Architecture Framework* and helps resolve the information-processing and usage problems identified by the 9/11 Commission. ISE Shared Spaces are networked data and information repositories used by ISE participants to make their standardized terrorism-related information, applications, and services accessible to other ISE participants. ISE Shared Spaces also provide an infrastructure solution for those ISE participants with national security system (NSS) network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Additionally, ISE Shared Spaces also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts. For more information about the ISE Shared Spaces concept, reference the *ISE Enterprise Architecture Framework* and the *ISE Profile Architecture and Implementation Strategy* at www.ise.gov.

ISE-Suspicious Activity Report (ISE-SAR)
An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

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 Assessment
A comprehensive report on an intelligence issue related to criminal or national security threats available to federal, state, local, and tribal law enforcement agencies.

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

Intelligence Community
Agencies of the U.S. government identified by statute and Executive Order, including intelligence elements of the U.S. Department of Defense, that have the responsibility to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national and homeland security of the United States. These activities include, in part, the collection of information and the production and dissemination of intelligence. (50 U.S.C. § 401a; Section 3 of the National Security Act of 1947, as amended; and Executive Order 12333.)

Intelligence Estimate
The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to criminal offenders and terrorists and the order of probability of their adoption. Includes strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue that is subject to analysis.

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

Intelligence Gap
An unanswered question about a cyber, criminal, or national security issue or threat.

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

Intelligence-Led Policing
The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses.

Intelligence Mission
The role that the intelligence function of a law enforcement agency fulfills in support of the overall mission of the agency; it specifies in general language what the function is intended to accomplish.

Intelligence Officer
A law enforcement officer assigned to an agency's intelligence function for the purposes of investigation, liaison, or other intelligence-related activity that requires or benefits from having a sworn officer perform the activity.

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 (Files)
Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts or are suspected of being or having been involved in criminal activities with known or suspected crime figures.

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.

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

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 facilitates information sharing among partner agencies.

Key Word In Context (KWIC)
An automated system that indexes selected key words that represent the evidence or information being stored.

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.

Methods
These are the methodologies (e.g., electronic surveillance or undercover operations) of how critical information is obtained and recorded.

Money Laundering
The practice of using multiple unlawful transactions of money and/or negotiable instruments gained through illegal activities with the intent of hiding the origin of the income, those who have been "paid" from the income, and/or the location of the unlawful income.

National Central Bureau (NCB or USNCB)
The United States NCB headquarters (INTERPOL) is located in Washington, DC.

National Criminal Intelligence Resource Center (NCIRC)
An Internet Web site that contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized resource information bank to access a multitude of criminal intelligence resources to help law enforcement agencies develop, implement, and retain a lawful and effective intelligence capacity.

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

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 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 Joint Terrorism Task Force
A joint entity led by the FBI and composed of over 40 agencies and established to enhance communication, coordination, and cooperation among federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security community by providing a point of fusion for the sharing of terrorism threats and intelligence; to provide operational support to the Counterterrorism Division; and to provide program management, oversight, and support for the JTTFs throughout the United States.

National Preparedness Guidelines
The U.S. government's guiding document for all-hazards preparedness, issued October 2007. The Guidelines established a vision for national preparedness and provide a systematic approach for organizing, synchronizing, and prioritizing national (including federal, state, local, tribal, and territorial) efforts to strengthen national preparedness. The Guidelines are umbrella documents that collate many plans, strategies, and systems into an overarching framework, the National Preparedness System. The Guidelines were developed in response to the President's Homeland Security Presidential Directive 8 (HSPD-8) of December 17, 2003 (*"National Preparedness"*). The Guidelines adopt an all-hazards approach and facilitate a capability-based and risk-based investment planning process for preparedness.

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.

Open Communications (OPCOM)
The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for the purposes of analyzing the information.

Open Source Information (or Intelligence)
Individual data, records, reports, and assessments that may shed light on an investigatory target or event which does not require any legal process or any type of clandestine collection techniques for a law enforcement agency to obtain. Rather, it is obtained through means that meet copyright and commercial requirements of vendors, as well as being free of legal restrictions to access by anyone who seeks that information.

Operational Analysis
An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist.

Operational Intelligence
Information evaluated and systematically organized on an active or potential target, such as groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

Outcome Evaluation
The process of determining the value or amount of success in achieving a predetermined objective through defining the objective in some qualitative or quantitative measurable terms, identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective, determination and explanation of the degree of success, and recommendations for further program actions to attain the desired objectives/outcomes.

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.

Pointer System or Index
A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

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.

Prediction
The projection of future criminal actions or changes in the nature of crime trends or a criminal enterprise based on an analysis of information depicting historical trends from which a forecast is based.

Preventive Intelligence
Intelligence that can be used to interdict or forestall a crime or terrorist attack.

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.

Privacy Field
A data element that may be used to identify an individual and, therefore, may be subject to privacy protection. (ISE-SAR Functional Standard.)

Proactive
Taking action that is anticipatory to a problem or situation with the intent to eliminate or mitigate the effect of the incident.

Procedural Due Process
Mandates and guarantees of law that ensure that the procedures employed to deprive a person of life, liberty, or property, during the course of the criminal justice process, meet constitutional standards.

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.

Profile/Criminal Profile
An investigative technique used to identify and define the major personality and behavioral characteristics of the criminal offender based upon an analysis of the crime(s) he or she has committed.

Protected Information
Defined in the ISE Privacy Guidelines, Section 1.b.—For federal non-intelligence agencies and state, local, and tribal agencies, it means, at a minimum, personably identifiable information about U.S. citizens and lawful permanent residents. States can extend this definition to other classes of persons or to all persons (including organizations).

Protocol (of Intelligence Collection)
Information collection procedures employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

Purging (Records)
The removal and/or destruction of records because they are deemed to be of no further value or further access to the records would serve no legitimate government interest.

Qualitative (Methods)
Research methods that collect and analyze information which is described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information.

Quantitative (Methods)
Research methods that collect and analyze information which can be counted or placed on a scale of measurement that can be statistically analyzed.

Racketeer Influenced and Corrupt Organizations (RICO) Act (or similar state statutes)
Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961–1968) provides civil and criminal penalties for persons who engage in a pattern of racketeering activity or collection of an unlawful debt that has a specified relationship to an enterprise that affects interstate commerce.

Racketeering Activity
State felonies involving murder, robbery, extortion, and several other serious offenses and more than 30 serious federal offenses, including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

Reasonable Suspicion
The existence of information that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

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

Records (Intelligence)
See Intelligence Records (Files).

Records System
A group of records from which information is retrieved by reference to a name or other personal identifier, such as a social security number.

Regional Information Sharing Systems® (RISS)
RISS is composed of six regional intelligence centers that provide secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to more than 8,000 federal, state, local, and tribal member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

Regional Intelligence Centers
Multijurisdictional centers cooperatively developed within a logical geographical area that coordinate federal, state, and local law enforcement information with other information sources to track and assess criminal and terrorist threats that are operating in or interacting with the region.

Reliability
Asks the question, "Is the source of the information consistent and dependable?"

Reporting
Depending upon the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption.

Requirements (Information or Intelligence)
The types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations in order for law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

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

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

Risk is classically represented as the product of a probability of a particular outcome and the results of that outcome. A statewide or regional assessment of the threats, vulnerabilities, and consequences faced by the fusion center's geographic area responsibility. The risk assessment is used to identify priority information requirements for the fusion center and to support state and urban area homeland security preparedness planning efforts to allocate funding, capabilities, and other resources.

In traditional criminal intelligence, a risk assessment means an analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

Risk Management-Based Intelligence
Risk management is a continual process or cycle in which risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and avoidance.

An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policymaking, especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability, or modality; can be quantitative if a proper database exists to measure

likelihood and impact and calculate risk; can be qualitative and subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations.

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.

Sealing (Records)
Records stored by an agency that cannot be accessed, referenced, or used without a court order or statutory authority based on a showing of evidence that there is a legitimate government interest to review the sealed information.

Sector Coordinating Councils (SCCs)
Serve as the government's principal point of entry into each sector for the purpose of addressing the entire range of CIKR protection and risk management issues. While they are supported and facilitated by DHS and the sector-specific agency, SCCs are self-organized, self-governed entities composed of a broad base of sector infrastructure owner-operators and their representatives from sector trade associations. Often chaired by a sector owner-operator, SCCs serve as "honest brokers" to facilitate sector-wide organization and coordination of a sector's CIKR protection policy development, planning, and program implementation and monitoring activities. Each SCC identifies, coordinates and supports the information sharing principles, needs, and capabilities most appropriate for its sector as required by HSPD-7.

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.)

Sensitive Compartmented Information (SCI)
Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems.

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

Sensitive Homeland Security Information (SHSI)
Any information created or received by an agency or any local, county, state, or tribal government that the loss, misuse, unauthorized disclosure, modification of, or the unauthorized access to could reasonably be expected to significantly impair the capabilities and/or efforts of agencies and/or local, county, state, and tribal personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. SHSI does not include any information that is:

1. Classified as national security information pursuant to Executive Order 12958, as amended, or any successor order.
2. Designated by Executive Order 12951, any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure.
3. Protected Critical Infrastructure Information (PCII) as defined in 6 CFR Part 29.2.
4. Sensitive Security Information (SSI) as defined in 49 CFR Part 1520.

Shared Spaces or Shared Space Concept
See ISE Shared Spaces Concept

Sources
From an intelligence perspective, these are persons (human intelligence, or HUMINT) who collect or possess critical information needed for intelligence analysis.

Spatial Analysis
The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity.

Statistical System
An organized means of collecting, processing, storing, and retrieving aggregate information for the purposes of analysis, research, and reference. No individual records are stored in a statistical system.

Strategic Intelligence
An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for the purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

Substantive Due Process
Guarantees persons against arbitrary, unreasonable, or capricious laws and acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

Surveillance
The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information, or "lead" information, which is used for the furtherance of a criminal investigation.

Suspicious Activity
Reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention. (*Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, June 2008; and ISE-SAR Functional Standard version 1.0.)

Suspicious Activity Report (SAR)
Official documentation of reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention. (*Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, June 2008; and ISE-SAR Functional Standard version 1.0.)

Tactical Intelligence
Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

Target
Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

Target Capabilities List
A component of the *National Preparedness Guidelines*, which describe the collective national capabilities required to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Guidelines use a capabilities-based preparedness approach to planning. Simply put, a capability provides the means to accomplish a mission. Some capabilities cut across all mission areas and are therefore placed in a Common Mission Area. Relevant Target Capabilities for fusion centers include:

- Intelligence/Information Sharing and Dissemination (Common Mission Area)
- Risk Management (Common)
- Information Gathering and Recognition of Indicators and Warnings (Prevent)
- Intelligence Analysis and Production (Prevent)
- Counter-Terror Investigations and Law Enforcement (Prevent)
- Law Enforcement Investigation and Operations (Prevent)

In addition, some fusion centers' defined missions support other capabilities, such as:

- Critical Infrastructure Protection (Protect)
- Epidemiological Surveillance and Investigation (Protect)
- Food and Agriculture Safety and Defense (Protect)
- Emergency Public Information and Warning (Response)
- Public Safety and Security Response (Response)
- CBRNE Detection (Prevent)

Note on Using the *Target Capabilities List*—The *Target Capabilities List* should be viewed as a reference document or guide to preparedness. The TCL is available for review at www.llis.dhs.gov.

Target Profile
A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals.

Targeting
The identification of crimes, crime trends, and crime patterns that have discernable characteristics which make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

Tear-Line Report
A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the "tear line" can be released as sensitive but unclassified.

Telephone Record (Toll)/Communications Analysis
An assessment of telephone call activity associated with investigatory targets to include telephone numbers called and/or received, the frequency of calls between numbers, the dates of calls, length of calls, and patterns of use.

Third-Agency Rule
An agreement wherein a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency.

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.

Undercover Investigation
Active infiltration of or an attempt to infiltrate a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or lead information that is used for the furtherance of a criminal investigation.

Validity
Asks the question, "Does the information actually represent what we believe it represents?"

Variable
Any characteristic on which individuals, groups, items, or incidents differ.

Vet
To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts to ascertain the product's accuracy, consistency with philosophy, and/or feasibility before proceeding.

Violent Criminal Apprehension Program (VICAP)
A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

Vulnerability Assessment
An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

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.

Appendix C—Acronym List

AAG	Associate Attorney General
ABA	American Bar Association
ACA	American Correctional Association
ACJA	American Criminal Justice Association
ACLU	American Civil Liberties Union
ACS	Automated Case System (FBI)
ACTIC	Arizona Counter Terrorism Information Center
ADA	Assistant District Attorney (or Americans with Disabilities Act)
AFIS	Automated Fingerprint Identification System
AG	Attorney General
APB	Advisory Policy Board or All Points Bulletin
APPA	American Probation and Parole Association
ARJIS	Automated Regional Justice Information System
ASAC	Assistant Special Agent in Charge
ASCA	Association of State Correctional Administrators
ASCIA	Association of State Criminal Investigative Agencies
ATAC	Anti-Terrorism Advisory Council
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATIX	Automated Trusted Information Exchange™
ATTF	Anti-Terrorism Task Force (FBI)
AUSA	Assistant U.S. Attorney
BATFE	Bureau of Alcohol, Tobacco, Firearms and Explosives
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
BOP	Federal Bureau of Prisons
BSA	Bank Secrecy Act (FinCEN-related)
CAD	Computer-Aided Dispatch
CAT	Communities Against Terrorism
CALEA	Commission on Accreditation for Law Enforcement Agencies
CapWIN	Capital Wireless Integrated Network
CATIC	California Anti-Terrorism Information Center
CBP	U.S. Customs and Border Protection
CBR	Chemical, Biological, Radiological
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CCH	Computerized Criminal Histories
CDC	Centers for Disease Control
CenTF	Center for Task Force Training
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CI	Confidential Informant *or* Criminal Intelligence *or* Counter Intelligence (Intelligence Community)
CIKR	Critical Infrastructure and Key Resources
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
CICE	Criminal Intelligence for the Chief Executive
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Criminal Information Sharing Alliance
CISAnet	Criminal Information Sharing Alliance Network
CJIS	Criminal Justice Information Services
CJNet	Criminal Justice Network
CODIS	Combined DNA Index System
COI	Community of Interest
CompStat	Computerized Statistics

ConOps	Concept of Operations
COOP	Continuity of Operations Plan
COP	Community Oriented Policing
COPS	Office of Community Oriented Policing Services
COT	Committee on Terrorism (Intelligence Subcommittee)
CT	Counterterrorism
CTD	Counterterrorism Division (FBI)
CTR	Currency Transaction Report
CUI	Controlled Unclassified Information
DA	District Attorney
DAG	Deputy Attorney General
DEA	U.S. Drug Enforcement Administration
DELJIS	Delaware Justice Information System
DHHS	U.S. Department of Health and Human Services
DHS	U.S. Department of Homeland Security (or Defense HUMINT Service)
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DNI-U	Director of National Intelligence-Unclassified
DOC	Department of Corrections (or U.S. Department of Commerce)
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
DOR	Department of Revenue
DOS	U.S. Department of State
DOT	U.S. Department of Transportation
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOP	Executive Office of the President
EOUSA	Executive Office for United States Attorneys
EPA	Environmental Protection Agency
EPIC	El Paso Intelligence Center
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBI CJIS	FBI Criminal Justice Information Services Division
FCG	*Fusion Center Guidelines*
FEMA	Federal Emergency Management Agency
FI	Field Interview/Field Interview Card
FIAT	Foundations of Intelligence Analysis Training
FIG	Field Intelligence Group (FBI)
FinCEN	Financial Crimes Enforcement Network
FIP	Fair Information Practices
FIR	Field Interview Report
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FOUO	"For Official Use Only" information handling caveat
G.R.E.A.T.	Gang Resistance Education And Training
GAC	Global Advisory Committee
GAO	U.S. Government Accountability Office
GESC	Global Executive Steering Committee
GFIPM	Global Federated Identity Privilege Management
GHSAC	Governors Homeland Security Advisory Council
GIS	Geographic Information Systems
GIWG	Global Intelligence Working Group
GJXDM	Global Justice XML Data Model
Global	Global Justice Information Sharing Initiative
GPS	Global Positioning System
HIDTA	High Intensity Drug Trafficking Areas
HIDTA DIG	HIDTA's Digital Information Gateway
HIFCA	High Intensity Financial Crime Area
HIR	Homeland Information Report
HQ	Headquarters
HS	Homeland Security
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSDN	Homeland Secure Data Network
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
HSIN-CI	Homeland Security Information Network-Critical Infrastructure
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
IAIP	Information Analysis and Infrastructure Protection
IALEIA	International Association of Law Enforcement Intelligence Analysts
IC	U.S. Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
ICS	Incident Command System

III	Interstate Identification Index
IIR	Institute for Intergovernmental Research® *or* Intelligence Information Report
IJIS	Integrated Justice Information Systems
ILO	Intelligence Liaison Officer *or* Industry Liaison Officer *or* Infrastructure Liaison Officer
ILP	Intelligence-Led Policing
INTERPOL	International Criminal Police Organization
IRS	Internal Revenue Service *or* Intelligence Resource Specialist
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
ISE	Information Sharing Environment
ISE-SAR	Terrorism-Related Suspicious Activity Report
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JAG	Judge Advocate General or Justice Assistance Grant Program
JIEM	Justice Information Exchange Model
JRIES	Joint Regional Information Exchange System
JTTF	Joint Terrorism Task Force (FBI)
LEA	Law Enforcement Agency
LECC	Law Enforcement Coordinating Committee
LEIS	Law Enforcement Information Sharing Strategy
LEISP	Law Enforcement Information Sharing Program
LEIU	Law Enforcement Intelligence Unit
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive—information-handling caveat
LETPP	Law Enforcement Terrorism Prevention Program
LLIS	Lessons Learned Information Sharing
MAGLOCLEN	Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network®
MCC	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MIPT	Memorial Institute for the Prevention of Terrorism
MOCIC	Mid-States Organized Crime Information Center®
MOU	Memorandum of Understanding
NACIC	National Counterintelligence Information Center
NARA	U.S. National Archives and Records Administration
NCB	National Central Bureau (U.S. contact for INTERPOL)
NCIC	National Crime Information Center
NCIRC	National Criminal Intelligence Resource Center
NCIS	Naval Criminal Investigative Service *or* National Criminal Intelligence Service—UK
NCISP	*National Criminal Intelligence Sharing Plan*
NCJA	National Criminal Justice Association
NCSL	National Conference of State Legislatures
NCTC	National Counterterrorism Center
N-DEx	Law Enforcement National Data Exchange (FBI)
NDIC	National Drug Intelligence Center
NDPIX	National Drug Pointer Index
NESPIN	New England State Police Information Network®
NFCCG	National Fusion Center Coordinating Group
NGA	National Geospatial-Intelligence Agency *or* National Governors Association
NGB	National Guard Bureau
NGIC	National Gang Intelligence Center
NICC	National Infrastructure Coordinating Center
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIPC	National Infrastructure Coordination Center
NIPP	*National Infrastructure Protection Plan*
NJTTF	National Joint Terrorism Task Force
NLETC	National Law Enforcement Training Center
Nlets	Nlets—The International Justice and Public Safety Network
NOC	National Operations Center
NPD	National Preparedness Directorate
NRIG	Northeast Region Intelligence Group
NSA	National Sheriffs' Association *or* National Security Agency
NSD	National Security Directive
NSOPR	National Sex Offender Public Registry
NSOPW	National Sex Offender Public Website

NSOR	National Sex Offender Registry
NW3C	National White Collar Crime Center
ODNI	Office of the Director of National Intelligence
OEM	Office of Emergency Management
OJP	Office of Justice Programs
OMB	Office of Management and Budget
P3I	Public-Private Partnerships for Intelligence
PART	Program Assessment Rating Tool
PERF	Police Executive Research Forum
PKI	Public Key Infrastructure
PM-ISE	Office of the Program Manager, Information Sharing Environment
PPP	Public-Private Partnerships
RAC	Resident Agent in Charge
RCPI	Regional Community Policing Institute (of COPS)
R-DEx	Regional Data Exchange (FBI)
RFI	Request for Information
RFP	Request for Proposal
RFS	Request for Service
RISS	Regional Information Sharing Systems®
RISSafe™	RISS Officer Safety Event Deconfliction System
RISS ATIX™	RISS Automated Trusted Information Exchange
RISS DES	RISS Data Exchange Specification
RISSNET™	Regional Information Sharing Systems Secure Intranet
RMIN	Rocky Mountain Information Network®
RMS	Records Management System
ROCIC	Regional Organized Crime Information Center®
RTTAC	Regional Terrorism Threat Assessment Center
RTTF	Regional Terrorism Task Force (FBI)
SAA	State Administrative Agency
SAC	Special Agent in Charge
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Councils
SCI	(Top Secret) Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SEARCH	The National Consortium for Justice Information and Statistics
SEOC	State Emergency Operations Center
SHSI	Sensitive Homeland Security Information
SIG	Special Interest Group
SIPRNET	Secret Internet Protocol Router Network
SLATT®	State and Local Anti-Terrorism Training
SLT	State, Local, and Tribal
SOP	Standard Operating Procedure
SSA	Senior Special Agent (or Supervisory Special Agent)
TA	Technical Assistance
TCL	*Target Capabilities List* (DHS)
TC Project	Trusted Credential Project
TEW	Terrorism Early Warning Group
TLO	Terrorism Liaison Officer
TPEP	Terrorism Prevention Exercise Program (DHS)
TS	Top Secret
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TS/SCI	Top Secret/Special Compartmented Intelligence
UASI	Urban Areas Security Initiative
USA	United States Attorney *or* United States of America
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
USAO	United States Attorney's Office
USBP	United States Border Patrol
USC	U.S. Currency, U.S. Citizen, or United States Code
US-CERT	United States Computer Emergency Readiness Team (DHS)
USCG	United States Coast Guard
USMS	United States Marshals Service
USPS	United States Postal Service
USSS	United States Secret Service *or* United States Standards Strategy
VGTOF	Violent Gang and Terrorist Organization File
VICAP	Violent Criminal Apprehension Program
WMD	Weapons of Mass Destruction
WSIN	Western States Information Network®

Appendix D – Resources

Introduction

Purpose

Fusion Center Guidelines
http://www.iir.com/global/guidelines.htm

National Strategy for Information Sharing
http://www.whitehouse.gov/nsc/infosharing/index.html

Information Sharing Environment
http://www.ise.gov

Introduction and Background

Global Justice Information Sharing Initiative (Global)
http://www.it.ojp.gov/topic.jsp?topic_id=8

National Criminal Intelligence Sharing Plan (NCISP)
http://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf

NCISP with Resource Library
http://it.ojp.gov/documents/ncisp

Intelligence Reform and Terrorism Prevention Act of 2004
http://www.nctc.gov/docs/pl108_458.pdf

"Guidelines and Requirements in Support of the Information Sharing Environment," Presidential Memorandum for the Heads of Executive Departments and Agencies, December 16, 2005
http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

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

Fusion Center Capability Areas

I. Fusion Process Capabilities

A. Planning and Requirements Development

National Strategy for Information Sharing
http://www.whitehouse.gov/nsc/infosharing/index.html

Joint Terrorism Task Forces
http://www.usdoj.gov/jttf

High Intensity Drug Trafficking Areas
http://www.whitehousedrugpolicy.gov/hidta

Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project
Available in fall 2008.

Major Cities Chiefs Association
http://www.majorcitieschiefs.org

Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR)
http://www.ise.gov/docs/ctiss/ISE-FS-200SARFunctionalStandardIssuanceVersion1.0.pdf

Information Sharing Environment Enterprise Architecture Framework
http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf

Information Sharing Environment Profile and Architecture Implementation Strategy
http://www.ise.gov/docs/eaf/ISE-PAIS.pdf

National Integration Center (NIC) Incident Management Systems Integration Division
http://www.fema.gov/emergency/nims/index.shtm

National Incident Management System (NIMS) Incident Command System
http://www.fema.gov/pdf/nims/NIMS_basic_incident_command_system.pdf

U.S. Department of Homeland Security's *National Preparedness Guidelines*
http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf

Target Capabilities List (TCL)
https://www.llis.dhs.gov/docdetails/details.do?contentID=26724

Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers, an appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*
Available in fall 2008.

State, Local, Tribal, and Territorial Government Coordinating Council
http://www.dhs.gov/xprevprot/committees/gc_1177096698216.shtm

National Infrastructure Protection Plan (NIPP)
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

NIPP Resource Center
http://www.learningservices.us/DHS/NIPP

National Criminal Intelligence Resource Center (NCIRC)
http://www.ncirc.gov

Lessons Learned Information Sharing (LLIS) System
www.llis.dhs.gov

B. Information Gathering/Collection and Recognition of Indicators and Warnings

Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines*
www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf

C. Processing and Collation of Information

28 Code of Federal Regulation CFR Part 23
http://www.iir.com/28cfr/guideline.htm

Global Justice Information Sharing Initiative's *Analyst Toolbox*
https://it.ojp.gov/documents/analyst_toolbox.pdf

Law Enforcement Analytic Standards
http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf

D. Intelligence Analysis and Production

Law Enforcement Analytic Standards
http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf

Intelligence Analysis Training can be found at:
http://mastercalendar.ncirc.gov

Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States
http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf

Global Justice Information Sharing Initiative's *Analyst Toolbox*
https://it.ojp.gov/documents/analyst_toolbox.pdf

International Association of Law Enforcement Intelligence Analysts (IALEIA)
http://www.ialeia.org

E. Intelligence/Information Dissemination

National Information Exchange Model (NIEM)
http://www.niem.gov

F. Reevaluation

Program Assessment Rating Tool
http://www.whitehouse.gov/omb/expectmore/part.html

Fusion Process Capability Areas

II. Management and Administrative Capabilities

A. Management/Governance

Fusion Center Guidelines
http://it.ojp.gov/documents/fusion_center_guidelines.pdf

B. Information Privacy Protections

ISE Privacy Guidelines—*"Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment"*
http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf

28 CFR Part 23 Criminal Intelligence Systems Operating Policies
http://www.it.ojp.gov/documents/28CFR_Part_23.pdf

Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment
http://www.ise.gov/docs/privacy/PrivacyImpGuide.pdf

Privacy and Civil Liberties Policy Development Guide and Implementation Templates
https://it.ojp.gov/documents/Privacy_Guide_Final.pdf

C. Security

Applying Security Practices to Justice Information Sharing
http://it.ojp.gov/documents/asp/ApplyingSecurityPractices.pdf

49 CFR Part 1520
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title49/49cfr1520_main_02.tpl

Enter title number 49, and search for Part 1520.

Protected Critical Infrastructure Information (PCII) Regulations Final Rule: Procedures for Handling PCII
http://www.dhs.gov/xinfoshare/laws/gc_1158333877680.shtm

Chemical-terrorism Vulnerability Information (CVI)
http://www.dhs.gov/xprevprot/programs/gc_1181835547413.shtm

D. Personnel and Training

Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States
http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf

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

Fusion Center Business Architecture
Available in fall 2008.

U.S. Department of Homeland Security Office of Infrastructure Protection
http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm

F. Funding

Grants.gov
www.grants.gov

DHS Homeland Security Grant Program (HSGP)
www.fema.gov/grants

Other

Executive Order 12958—Classified National Security Information, as Amended
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid=fr20ap95-135.pdf

"Designation and Sharing of Controlled Unclassified Information (CUI)"
Presidential Memorandum for the Heads of Executive Departments and Agencies, May 9, 2008
http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html

Executive Order 12951—Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid=fr28fe95-133.pdf