Global Justice Information Sharing Initiative
United States
Department of Justice

Defining Fusion Center Technology Business Processes: A Tool for Planning

DHS/DOJ Fusion Process Technical Assistance Program and Services

April 2009

Defining Fusion Center Technology Business Processes: A Tool for Planning

DHS/DOJ Fusion Process
Technical Assistance
Program and Services

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

Foreword

The U.S. Department of Justice's (DOJ) and the U.S. Department of Homeland Security's (DHS) joint DOJ/DHS Training and Technical Assistance program collaborated in the development of this business process tool for fusion centers.

The initial project was launched in November 2006 with the idea of documenting the business and technical architecture for fusion centers. The IJIS Institute (IJIS) was designated as the lead facilitator, with the Institute for Intergovernmental Research® (IIR), SEARCH—The National Consortium for Justice Information and Statistics, and the National Center for State Courts (NCSC) in support. A working group was identified consisting of industry representatives and staff from IIR, SEARCH, NCSC, and IJIS with expertise in business and technical architecture. Very early in the project, it was determined that attempting to create a single-standard technical architecture applicable to all fusion centers was not feasible due to the variances of technical infrastructure, tools, capabilities, and methodologies that are or would be in use among the fusion centers. Therefore, the working group focused its attention on business architecture.

During the course of drafting a document on fusion center business architecture, it was realized that, similar to the technical architecture, the business architecture is also inherently diverse. Business architecture differs among fusion centers due to variations regarding governance, command structure, operational divisions, stakeholders, customers, and target capabilities. However, a critical need exists in assisting fusion centers with the formulation of their business architecture. Many fusion centers are just beginning to plan for or implement the processes to handle the many capabilities that are assigned to them. Once the business processes are defined, the fusion center is in a much better position to purchase or develop technology to handle those processes. Therefore, the working group turned its efforts to create a tool that any fusion center could use to assist in the creation and documentation of its own business processes. This tool consists of a methodology for creating and documenting business processes, templates for both the process and capabilities that support the process, and important reference material. While this effort was in progress, the working group was expanded to include four fusion center practitioners to provide additional review and perspective.

This effort would not have been possible without the support and guidance of key individuals. A special thank-you is given to the following individuals for their leadership and commitment to this initiative:
Gerry Wethington, Unisys; Thomas O'Reilly, Bureau of Justice Assistance; Scott Came, SEARCH;
Lorraine Cimino, Apogen Technologies;
Robert Cummings, IIR; Chuck Dodson, Oracle Corporation; Scott Fairholm, NCSC; Kael Goodman, GovCore Solutions; Bill Kellett, Microsoft;
Scott Parker, IJIS; Philip Ramer, IIR; Sharad Rao,

Tetrus Consulting; Karma Temple, SRA International, Robert Wolf, Convergence; and Martin Zaworski, Unisys. Their collective knowledge, insight, and willingness to participate resulted in an outstanding product.

A thank-you is also extended to the following partner organizations for their efforts: the IJIS Institute (IJIS); the Institute for Intergovernmental Research (IIR); the National Center for State Courts (NCSC); and SEARCH—The National Consortium for Justice Information and Statistics.

Defining a Fusion Center

According to the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's (Global) *Fusion Center Guidelines*, "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* (Strategy) and is a key step to reaching one of the Strategy's goals of "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.

Purpose

The purpose of this document is to provide a tool to fusion center directors/managers to assist with understanding and implementing the fundamental business requirements of the center and planning for the underlying components for each of the business processes the particular fusion center is or will be undertaking (e.g., SAR process, training, and statewide incident analysis). It is essential that each center fully define its business processes before attempting to purchase or develop technology to handle those processes. If these processes are not clearly defined, the result will be that the technology will drive the business process rather than the business process driving the technology. Building upon strategic planning activities completed during the Fusion Center Concept of Operations (CONOPS) Development Technical Assistance service[1] and using the methods outlined in this document, directors/managers will be able to better define, understand, and articulate each process. As the processes are further defined, technology acquisition (if needed) and implementation can be more aligned with business needs.

Since fusion center processes and procedures vary greatly from one center to another, this business architecture framework is presented to enable an individual fusion center to analyze and map out its own business processes and thereby provide the fusion center with a road map to its own fully integrated business architecture. This framework provides a business model for fusion center processes utilizing the roles and responsibilities of local, state, tribal, and federal authorities as outlined in the *National Strategy for Information Sharing*. It takes these identified capabilities and information contained in several other valuable documents that have been published since the introduction of fusion centers and ties all the information together in regards to a business architecture model. This document supplies a methodology and templates for analyzing business architecture and includes example architecture models for two fusion center business processes—Suspicious Activity Reporting (SAR) and Incident Data Collection and Analysis.

This document builds on previous strategic planning initiatives and offers:

- A methodology and framework that assist fusion centers in further defining the business processes for their mission-critical services.
- A list of key considerations for launching or enhancing fusion center processes, including identification of potentially helpful technologies.

[1] A CONOPS is the core strategic document that synchronizes every facet of the fusion center. An effective CONOPS enables a fusion center to coordinate current operations while planning for the success of future operations. The Fusion Center CONOPS Development Technical Assistance service assists state and local fusion centers in developing the CONOPS document.

- A reference list of documents that supply key information to fusion centers.
- Business architecture framework examples for two typical business processes (Suspicious Activity Reporting and Incident Data Collection and Analysis).

This document does not:

- Solve the technical issues with which each agency and jurisdiction may be challenged.
- Mandate how a fusion center or partner should implement its processes or capabilities.
- Offer a recommended governance structure.
- Guarantee funding acquisition.
- Replace or supersede documents such as the *Fusion Center Guidelines*.

Target Audience

This document and its referenced business architecture framework templates are designed to serve fusion center managers, administrators, and implementers. This very large network of prospective readers includes leaders from local, state, tribal, and federal agencies as well as specific private entities.

Although many fusion centers were originally introduced to aid in information sharing and incident management for terrorist activity, that mission quickly expanded in most states and urban areas to include what many call the "all-crimes, all-threats, and all-hazards" approach. That means fusion center information gathering, analysis, and dissemination include communication with entities involved in support of counterterrorism, critical incidents, or both, with the inclusion of all crimes.

The challenge confronting all fusion center managers is to be responsive to the agencies contributing to and consuming information generated by the fusion center. There are a number of fusion center drivers, and being responsive to those drivers ultimately affects how fusion center managers interact with their clients. As previously stated, fusion centers can be structured to address many types of incidents: "all-threats," "all-crimes," "all-hazards," or strictly terrorism-based threats. Depending on the focus of the fusion center, the participants may be different. The participants can change with the focus as well as with the level of government from which they operate. For example, it is likely that in an all-terror center, one would encounter a number of federal agencies as well as a number of state agencies, mostly from the Intelligence Community, law enforcement, and homeland security. In an "all-hazards" operation, the participants may significantly expand to include agencies such as fire, emergency management, agriculture, transportation, and health, in addition to the more traditional public safety agencies. Understanding your clientele is extremely important when making decisions relative to what service offerings will make up your core capabilities. Finally, involving the appropriate participants in the design effort of your fusion center is also essential if you are going to be truly effective in implementing core capabilities and service offerings that can be effectively offered because (1) the data exists to support the offering and (2) the offering meets the information needs of the fusion center constituents.

Expected Benefits

Traditional information sharing methods among public safety, intelligence, and emergency management agencies no longer meet the information needs for those communities. Over the last several years, we have learned hard lessons from terrorist, natural disaster, and criminal events. We have learned that an information sharing network must be built and maintained to support the increasingly "elastic boundaries" of resources to include people, assets, and information. These boundaries must be able to stretch, expand, and continuously evolve in order to handle real-time situations, thus the scope of information sharing necessarily extends beyond the traditional systems involved in reactive public safety and criminal justice. Being prepared to react in real time necessitates being proactive not only in the preparation but prescriptive in the information needs, their uses, and expected advantages before needs arise. Today's environment has replaced the old model of "respond and recover" with a much-needed model of "prevent, protect against, respond to, and recover from."

Fusion centers play a critical role within this new model and offer significant value to our nation, local jurisdictions, and citizens within our communities. Value is often stated in a variety of ways. With the advent of fusion centers, it is extremely important to plan for the development of performance measures—particularly measures that can effectively articulate outcomes. While it is important to know how many agencies contribute to a fusion center; how many records are contained in a fusion center; how many leads are generated from a fusion center; and how often the leads assist in terrorism prevention, all-hazard mitigation, or crime reduction, it is perhaps more important to understand the answer to the question: “So what?” That is the value of outcomes; they provide a clear response to “what” difference fusion centers are making to enhance public safety and ultimately help to formulate the business case to support continued investment in fusion center operations. It is intended that through the adoption and use of this national fusion center business architecture framework, tangible benefits (such as those outlined in Table 1—Benefits of Documenting Business Processes) to fusion centers and their various partner agencies will be positively established.

Table 1—Benefits of Documenting Business Processes

Strategic Activity	Tangible Benefit	Resulting Outcomes
Multijurisdictional/ multiagency collaboration.	Enables the entire fusion community to leverage resources from different agencies. Promotes efficiencies and enhances the potential for effectiveness.	Duplication of effort is reduced or eliminated. This equates to lower operational costs through a more efficient use of personnel and resources.
Create or enhance fusion center and partner information sharing in a manner consistent with other communities.	Enables future integration in an economical manner. Eliminates or reduces barriers that impede communication and intelligence development and exchange. Leverages current investments (across public safety and intelligence communities at each jurisdictional level) to offset cost and time. Affords opportunities for cross-agency and fusion center backup in situations where immediate resources are unavailable or insufficient.	Increased efficiencies in gathering critical investigative information. Analysts and investigators are able to access a broad range of information from a variety of sources, which lends itself to lowering the economic cost of crime through the sharing of common resources and the enhanced ability to prevent cross-jurisdictional crime.
Facilitate the processing and collation of disparate data.	Enables data captured from different sources to be organized in a manner that makes it useful for investigative and analytical purposes. Information is easily synthesized in support of tactical initiatives.	The ability to aggregate data from a variety of sources provides a broader foundation for analysis and decision making; better analysis through access to more comprehensive data should result in higher rates of detection, clearances, and prevention of multijurisdictional crime and potential terrorist threats.
Application of analysis techniques enabled by advanced analytical tools.	Enables analytical services, such as crime pattern analysis, association analysis, telephone-toll analysis, flowcharting, financial analysis, and strategic analysis. Analysts are able to describe, understand, and map criminality and the criminal business process. Provides information to engage the most appropriate tactics.	Enables informed decisions and offers better choices for decision makers. Enables the targeted and better use of resources, thus enhancing efficiencies. Disrupts prolific criminals and terrorist threats through targeted decision making.

Reference Documents for Fusion Centers

A significant number of reference materials exist relative to the operational support of fusion centers and their local, state, tribal, and federal partners. Although this is not a complete list of those reference documents, the following table provides a minimal list of key materials that should be used or considered during the formulation of fusion center business architecture and/or business processes.

Table 2—Reference Documents

Document	Key Usage	Host Web Site
Baseline Capabilities for State and Major Urban Area Fusion Centers	This document identifies the full spectrum of minimum baseline capabilities fusion centers should achieve. It serves as a companion document to the U.S. Department of Justice's Global Justice Information Sharing Initiative's (Global) *Fusion Center Guidelines* by outlining the minimum capabilities state and major urban area fusion centers should include in their operations. It identifies elements that serve as the foundation for integrating state and major urban area fusion centers into the national Information Sharing Environment (ISE) and ensuring continuity and sustainability of fusion center operations at the state and local levels.	www.it.ojp.gov/documents/baselinecapabilitiesa.pdf
National Strategy for Information Sharing	Appendix 1 of this document defines key capabilities for fusion centers.	http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html
Fusion Center Guidelines	This document defines the services performed by fusion centers.	http://it.ojp.gov/documents/fusion_center_guidelines.pdf
Target Capabilities List (TCL)	The *Target Capabilities List* (TCL) establishes an all-hazards framework. The TCL is a national-level, generic model of operationally ready capabilities defining all-hazards preparedness. Users should refer to the TCL to assess capabilities, identify needs, and inform plans and strategies, taking into account their risk. It is important to understand that the TCL serves as a reference document and planning guide to preparedness and in no way serves as a prescription for program or resource requirements.	https://www.llis.dhs.gov/docdetails/details.do?contentID=26724

Document	Key Usage	Host Web Site
National Criminal Intelligence Sharing Plan (NCISP)	This document outlines specific "action steps" related to criminal intelligence information sharing that can be taken immediately by almost any agency and what can be expected by performing those steps.	http://it.ojp.gov/documents/ncisp/
Justice Reference Architecture (JRA)	The JRA provides reference architecture with guidance for identifying, defining, implementing, and governing services for justice and public safety.	http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015
Law Enforcement Analytic Standards	This document defines standards for law enforcement analysts and analysis, based on the intelligence process or cycle.	https://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf
LEIU *Criminal Intelligence File Guidelines*	These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations.	http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf
Information Sharing Environment Enterprise Architecture Framework (ISE-EAF)	The ISE outlines the enterprise architecture framework for sharing terrorism information among all appropriate local, state, tribal, and federal entities and the private sector through the use of policy guidelines and technologies.	www.ise.gov/pages/eaf.html
Information Sharing Environment Implementation Plan (ISE-IP)	The ISE outlines the plan to provide and facilitate the means for sharing terrorism information among all appropriate local, state, tribal, and federal entities and the private sector through the use of policy guidelines and technologies.	http://www.ise.gov/docs/reports/ise-impplan-200611.pdf
Information Sharing Environment Privacy Guidelines	These guidelines 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
Common Terrorism Information Sharing Standards (CTISS) Program Manual	This document was developed to assist local, state, tribal, and federal governments in addressing the standardization of processes and products across the ISE community.	http://www.ise.gov/docs/ctiss/CTISSprogramManual20071031.pdf
28 CFR Part 23	The 28 Code of Federal Regulations (CFR) Part 23 is a guideline for law enforcement agencies. It contains implementing standards for operating federally funded multijurisdictional criminal intelligence systems. It applies to systems operating through federal funding under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.	http://www.iir.com/28cfr/guideline.htm
National Preparedness Guidelines	Homeland Security Presidential Directive 8 (HSPD-8) of December 17, 2003, directed the Secretary of Homeland Security to develop a national domestic all-hazards preparedness goal. The *National Preparedness Guidelines* finalize development of the national preparedness goal and its related preparedness tools.	http://www.dhs.gov/xprepresp/publications/gc_1189788256647.shtm
Minimum Criminal Intelligence Training Standards	The intent of this document is to provide perspective and guidance for the development and delivery of law enforcement intelligence training.	http://www.iir.com/global/products/minimum_criminal_intel_training_standards.pdf
DHS/FEMA *Technical Assistance: Preparedness & Program Management Technical Assistance Catalog*	The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), National Preparedness Directorate, Capabilities Division (CD), Technical Assistance (TA) program seeks to build and sustain capabilities through specific services and analytical capacities across two primary functional areas: preparedness technical assistance activities in support of the four homeland security mission areas (prevention, protection, response, and recovery) and homeland security program management.	http://www.ojp.usdoj.gov/odp/docs/NPD_Technical_Assistance_Catalog.pdf
ISE-FS-200 IEPD (ISE-SAR IEPD)	Suspicious Activity Reporting (SAR) Information Exchange Package Documentation (IEPD) for exchanges between the state-designated fusion center and the Information Sharing Environment (ISE).	http://www.ise.gov *(search for "SAR")*

Core Capabilities

Fusion center capabilities form the basis for the templates used for each business process evaluated. The capabilities listed below in the Fusion Process Capabilities and Management and Administrative Capabilities sections are extracted from the *Baseline Capabilities for State and Major Urban Area Fusion Centers* document. The Baseline Capabilities document contains much greater detail on each of the capabilities and should be utilized as the "master" list.

Depending upon the focus of the fusion center (i.e., "all terror," "all crimes," and/or "all hazards") and the consumer and contributor makeup of the fusion center's constituents, it is very likely that some service offerings may extend beyond those capabilities outlined below. Individual fusion centers may identify and define capabilities in addition to those listed, depending on the business process in question, that are necessary in order to achieve their stated mission (listed in the Noncategorized/Optional Capabilities section below). Clearly, it is important to keep in mind the business objectives of the fusion center and then develop those capabilities most suited to help the fusion center manager achieve the success outlined by the fusion center's vision and mission.

Fusion Process Capabilities

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

Section B: Information Gathering/ Collection and Recognition of Indicators and Warnings

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.
2. **Feedback Mechanism**—Fusion centers shall define and implement a feedback mechanism.
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.

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

Section 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 Assessment; 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.
2. **Management of the Analytic Function**—The analytic function in a fusion center should, when possible, be supervised or managed by personnel with previous analytic experience and with analytic management training.
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.
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.
5. **Strategic Analysis Services**—Fusion centers shall develop the capability to provide strategic analysis services for the jurisdiction served.
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.

Section 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.
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.
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.

Section 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.

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: [see the requirements set forth in the Baseline Capabilities document].

Management and Administrative Capabilities

Section 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.
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.
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.
4. **Policies and Procedures Manual**—Fusion centers shall develop a policies and procedures manual for center operations.
5. **Center Performance**—Fusion centers shall define expectations, measure performance, and determine effectiveness of their operations.
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.

Section 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.
2. **Privacy Policy Development**—In developing the privacy policy, fusion centers shall [meet the requirements set forth in the Baseline Capabilities].
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*.
4. **Privacy Policy Outreach**—Fusion centers shall implement necessary outreach and training for the execution, training, and technology aspects of the privacy protection policy.
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.

Section 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.
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.
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.

Section 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.
2. **Background Checks—**Ensure that background checks are conducted on center personnel (whether private or public) prior to the commencement of duties.
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.

Section 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.
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.
3. **Communications Plan**—Fusion centers shall have a plan to ensure safe, secure, and reliable communications, including policies and audit capabilities.
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, performance of essential functions at an alternate location during an emergency.

Section 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.

Noncategorized/Optional Capabilities[2]

1. The fusion center may provide support to law enforcement within its jurisdiction as appropriate. Potentially, this could take many forms. Some examples are Identity Confirmation, Gang Activity information, Narcotics Trafficking information, Interstate Crime Activities information, and Special Capabilities Resource List (Bomb Disposal, Bomb Detection K9s, Tracking K9s, etc.).
2. The fusion center may also provide support to public safety agencies/ activities within its jurisdiction, as appropriate. Potentially, this could take many forms. Fusion centers looking to explore these options should evaluate their needs and seek out appropriate expertise (e.g., DHS FEMA) to support their planning efforts. Some examples are Evacuation Plan Management, Mutual Aid Plans, Statewide Fire and EMS Equipment Inventories, Search and Rescue Resource List, and Additional Response and Recovery Mission Capabilities.

[2] These capabilities are not identified in the *Baseline Capabilities for State and Major Urban Area Fusion Centers.*

Creating the Business Architecture Framework

The architecture framework for fusion centers begins with the Enterprise Architecture (EA) Framework. Although all components are equally important considerations as they provide the rules and form factors to create the plan for services and information integration, this document focuses on the business architecture.

> *Business architecture provides a high-level representation of the business strategies, intentions, functions, processes, information, and assets critical to providing services to, in our case, the fusion center "customers"—local, state, tribal, and federal agencies and the private sector.*

The detail captured within the business architecture supports business decision making by providing documentation of where the enterprise is today and where the enterprise wants to be at a specified time in the future. Business architecture can be viewed as the foundation or driver for the other components of an enterprise architecture, ultimately the foundation for investment decisions in complementary technologies. For enterprise architecture to be successful, it must be linked to the business direction of the agency or center objectives. Business architecture must also consider interaction with other government units, as well as the delivery of services.

The fusion center information sharing framework is presented here via framework templates. The steps are:

1. Describe a Business Process
   a. Map Business Processes
   b. Identify Associated Capabilities
2. Create a Template for Each Associated Baseline Capability
3. Flowchart the Process

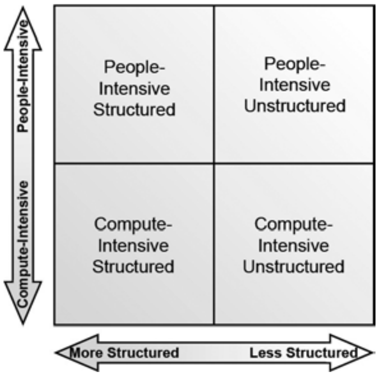
Two examples of the framework templates can be found in Appendix 1 of this document.

Step 1—Describe a Business Process

Specific fusion center business processes will vary from center to center, due to particular goals and objectives, local mandates, governance, threat assessments, and other considerations such as geographic characteristics, critical infrastructure types, resources, and funding availability.

The template on the next page assists in organizing the business process information.

Table 3—Process Template

Process Description		
Process Name	Name of the business process.	
Description	The description should be as specific as possible to distinguish from other processes and to allow readers to enter at any point in the architecture blueprint and understand the content of each component. A minimum of one paragraph should be written for the description.	
Rationale	The fundamental reason or basis for this process being included within the architecture. Rationale can be thought of as the motivation or reasoning that defines why the process is important to the enterprise. The rationale can include the major issues this process is to address or criteria used to guide the design of subordinate assets in the architecture blueprint. A minimum of one paragraph or three bulleted items should be written to describe the rationale.	
Benefits	The initial benefits associated with the process. These should be tangible, measurable outcomes that explain what the process will do for the enterprise. Benefits are best defined as the positive consequences entities can expect to receive from adopting or following the architecture blueprint assets defined within this process. A minimum of one paragraph or three bulleted items should be written to describe the benefits.	
Business Needs	 People-Intensive Structured People-Intensive Unstructured Compute-Intensive Structured Compute-Intensive Unstructured People-Intensive Compute-Intensive More Structured Less Structured	
Associated Baseline Capabilities	Identifies related business capabilities—i.e., list which capabilities are required for this process (see Section 3.1 for a listing of the Baseline Capabilities).	
Audit	Current Status	Document the status of this template, indicating whether it is in development, under review, approved, or rejected.
	Creation Date	Provide the date the process was created.
	Date Approved/Rejected	Provide the date the process was accepted into the architecture or rejected.
	Reason for Rejection	If the process was rejected, document the reason for the rejection.
	Last Date Reviewed	Document the most recent date the process was taken through the architecture process.
	Last Date Updated	Document the most recent date that any item in the process template was changed.
	Reason for Update	Document the reason for the update to the process.

The items included in the process description template are somewhat self-explanatory, except for the business needs graph and the associated capabilities, which are described further below.

Map Business Process

Fusion center business processes encompass a wide range of needs. The horizontal axis of this graph lays out a spectrum of business processes that range from highly structured to completely unstructured. The vertical axis lays out a spectrum of business processes that range from compute-intensive (using mostly computer resources) to people-intensive (using mostly human gray matter). The graph is divided into four quadrants:

Compute-Intensive, Structured: These business processes are generally considered to be "scheduled reports." They run on a regular basis, often unattended, and produce information for the fusion center. One example would be a nightly/weekly/monthly process that gathers and collates crime statistics from many different sources and produces a trend report for the fusion center.

Compute-Intensive, Unstructured: Business processes in this quadrant are generally thought of as analysis. They require a great deal of computing horsepower to search many disparate data sources, but they are unstructured in the sense that a person is searching the data in ad hoc, unique ways. For example, a suspected terrorist might frequently use unusual words in his chat room communications (the names of Hawaiian birds, for example). The fusion center might want to do analysis across many data sources to look for others using these same terms.

People-Intensive, Structured: These business processes are generally called "human workflow." Computers may play a secondary role in these processes, but fusion center members provide most of the value via structured collaboration. One example of this type of business process would be the evaluation/escalation process for a Suspicious Activity Report.

People-Intensive, Unstructured: These processes involve ad hoc, people-centric collaboration that is generally termed a "virtual meeting." Computers play a secondary role by providing tools that enable virtual "presence" across time and distance. A Situation Briefing is an example of this type of process.

The fusion center architecture team needs to map business processes to appropriate product capabilities. To do this, begin by mapping the business process to the graph, as shown in Illustration 2.

Although only four examples are shown, they illustrate the process. As each business process is mapped to the graph, you will gain an idea of the type of capabilities that are needed to support it.

Illustration 1—Business Process Mapping

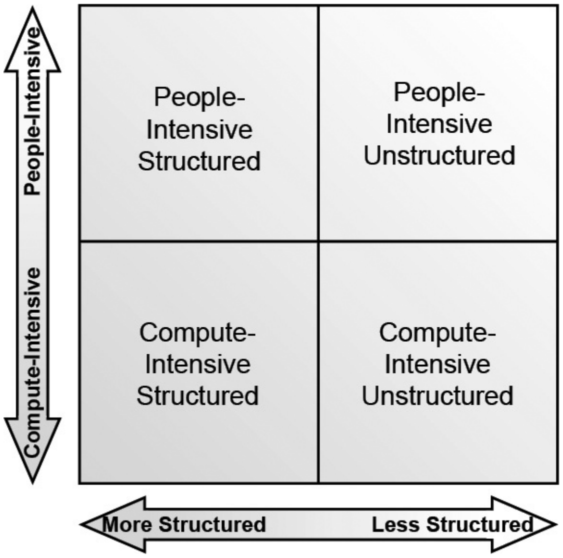
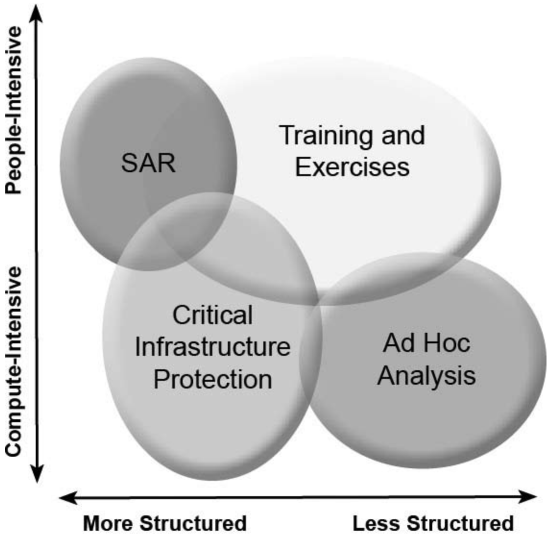

People-Intensive
Compute-Intensive
People-Intensive Structured
People-Intensive Unstructured
Compute-Intensive Structured
Compute-Intensive Unstructured
More Structured
Less Structured

Illustration 2—Business Mapping Examples



Identify Associated Baseline Capabilities

The fusion center and its many information sharing partners each offer specific services and capabilities. These services and capabilities will vary from center to center and are likely to extend beyond the capabilities enumerated in this document. Based on the process being examined, the capabilities that relate to the process should be fairly easily identified and listed. Use the core capabilities list as a starting place, and add any additional capabilities you may need for the particular business process.

Step 2—Create a Template for Each Associated Baseline Capability

Business architecture templates are included below for each capability. This template provides a standard method for describing each capability. Although these templates serve as a framework for the business architecture, it is expected they will be a starting point and will be modified to suit the particular fusion center's business needs. Much of the template is self-explanatory, although the reader can reference the examples in the appendix for further clarification.

Table 4—Capabilities Template

Capability Description		
Overview	Capability	Name of the capability.
	Description	The description should be as specific as possible to distinguish from other capabilities and to allow readers to enter at any point in the architecture blueprint and understand the content of each component. A minimum of one paragraph should be written for the description.
	Rationale	The fundamental reason or basis for this capability being included within the architecture. Rationale can be thought of as the motivation or reasoning that defines why the capability is important to the enterprise. The rationale can include the major issues this capability is to address or criteria used to guide the design of subordinate assets in the architecture blueprint. A minimum of one paragraph or three bulleted items should be written to describe the rationale.
	Benefits	The initial benefits associated with the capability. These should be tangible, measurable outcomes that explain what the capability will do for the enterprise. Benefits are best defined as the positive consequences entities can expect to receive from adopting or following the architecture blueprint assets defined within this capability. A minimum of one paragraph or three bulleted items should be written to describe the benefits.
	Associated Processes	Identifies related business processes—i.e., which processes does this capability support?
	Related Capabilities	List of other closely related capabilities.
Reference Documents	• List of reference documents and citations. Provide URLs for reference whenever possible.	
Standards and Governance	• Provide a list of the various standards and/or government bodies that affect this capability. Provide URLs for reference whenever possible.	
Stakeholders and Roles	Local Agencies	Describe the roles and responsibilities for this stakeholder. A minimum of one paragraph or three bulleted items should be written to describe the relationship.
	State Agencies	Describe the roles and responsibilities for this stakeholder. A minimum of one paragraph or three bulleted items should be written to describe the relationship.
	Federal Agencies	Describe the roles and responsibilities for this stakeholder. A minimum of one paragraph or three bulleted items should be written to describe the relationship.
	Other Fusion Centers	Describe the roles and responsibilities for this stakeholder. A minimum of one paragraph or three bulleted items should be written to describe the relationship.
	Private Sector	Describe the roles and responsibilities for this stakeholder. A minimum of one paragraph or three bulleted items should be written to describe the relationship.
Environmental Trends in Conflict	• List any capability-specific technology trends. Technology trends within the industry have an effect on the deployment of information technology. IT decision makers will develop more informed, effective decisions if they are aware of the impact of the technology trends. Also include mitigation tactics, if possible.	
Associated Compliance Components	• Provide a list of compliance components that are specific to the capability.	
Methodologies	• List methodologies to comply with compliance components followed in developing or supporting this capability as appropriate.	
Documentation Requirements	• Use this section to document the quality assurance criteria for the capability and express your expectations for how the capability is to be maintained.	
Associated Technology Areas	• Provide a list of the technology areas that are covered within this capability. This provides an index for these technology areas.	
Audit	Current Status	Document the status of this template, indicating whether it is in development, under review, approved, or rejected.
	Ranking/Priority	Fusion center ranking of priority of this capability as compared to other capabilities—provides a prioritization order for implementation.
	Creation Date	Provide the date the capability was created.
	Date Approved/ Rejected	Provide the date the capability was accepted into the architecture or rejected.
	Reason for Rejection	If the capability was rejected, document the reason for the rejection.
	Last Date Reviewed	Document the most recent date the capability was taken through the architecture process.
	Last Date Updated	Document the most recent date that any item in the capability template was changed.
	Reason for Update	Document the reason for the update to the capability.

Step 3—Flowchart the Process

The final step in creating a business architecture framework for a business process is the creation of a flowchart (process model). This step provides several benefits:

1. Provides a very good visual representation of your workflow and related components
2. Helps to identify contributing agencies (i.e., who is providing information)
3. Helps to identify consuming agencies (i.e., who is receiving information)

Many methods can be used for developing the flowchart:

- ✪ Unified Modeling Language (UML)
- ✪ Business Process Modeling Language (BPML) (reference: http://www.bpmi.org)

When creating the flowchart that represents the business process, consider the following:

> ***The identification of the contributing and consuming agencies is a key output of the business architecture process. Information sharing is the real strength of a fusion center, and the identification of these agencies is obviously a key component.***

Finished Framework

Once you have completed the template for the business process and templates for all associated capabilities and flowcharted the process, you have completed the business architecture for that business process.

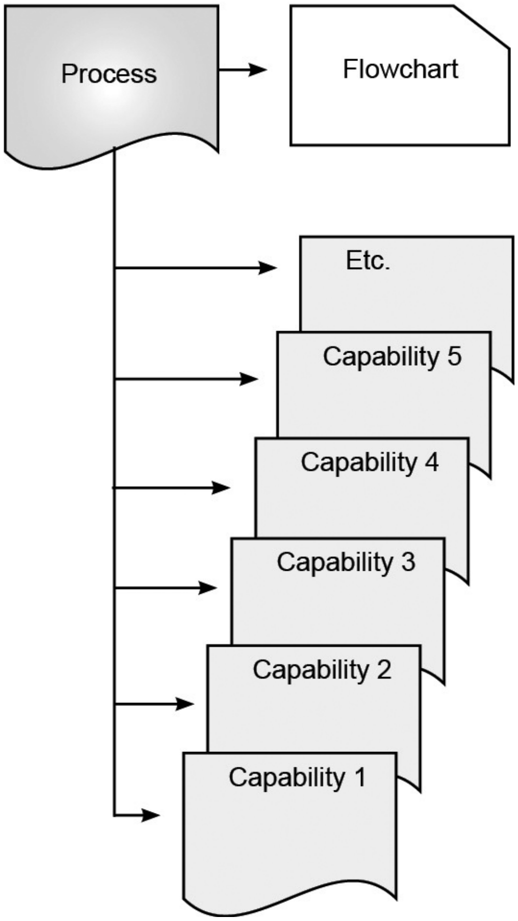
The business architecture templates should be reviewed and updated periodically because of changes in technology, priorities, and methodologies.

Consider placing the artifacts under a configuration management structure. Uniquely identify the artifacts, and determine the method of publication, review, and evolution.

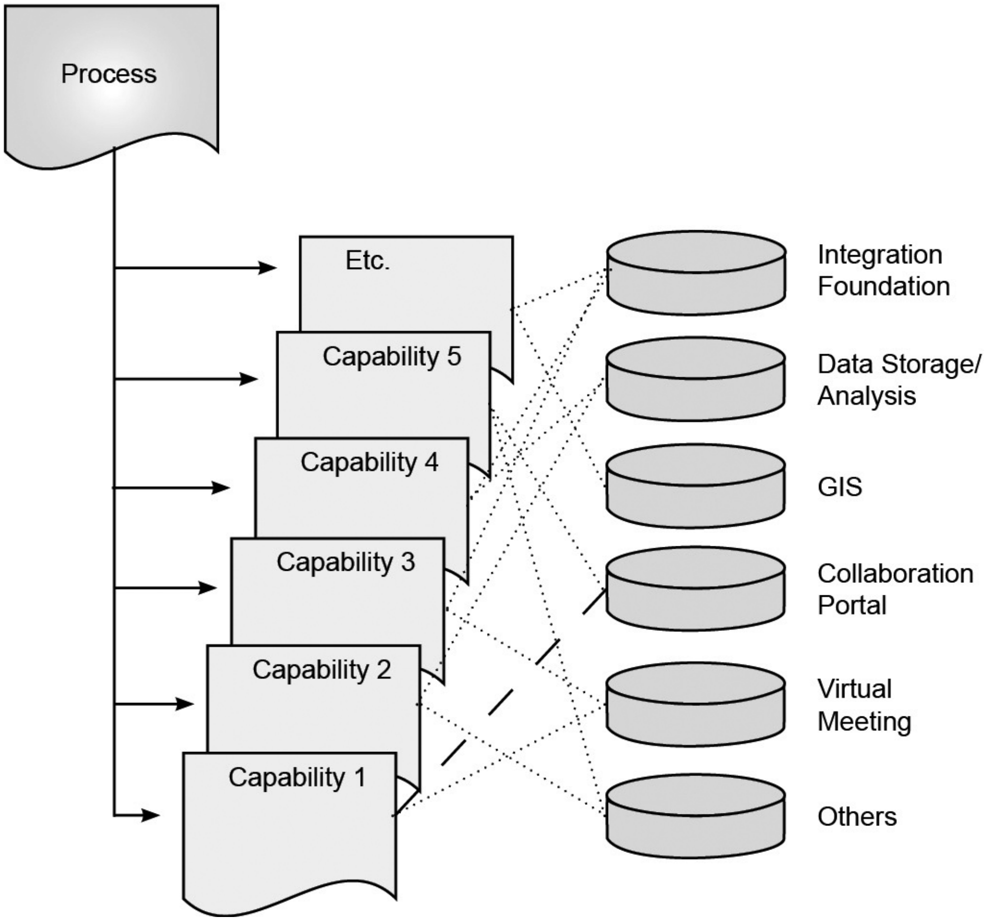
Table 5—Flowchart Considerations

Process Element	Questions to Consider	Examples
Inputs	Where is my information (data) coming from? What format is it going to be in? Who is providing the data? How often will they be providing the input?	Paper form inputs External database systems Internal database systems Phone call
Process Entry Criteria	What conditions must be met before the input data can be accepted? What types of validations must be satisfied prior to entering the business process?	Required data fields Agency and system identification Standardized format
Transformations	Does the input data need to be changed or reconfigured? How does the data need to be changed?	Data elements from source to destination (e.g., eye color) Data supplied in GJXDM/NIEM that must be transformed into the destination database
Processing	What business process needs to occur? What are the business rules that need to be satisfied?	Searching Comparison Analysis Collaboration
Process Exit Criteria	What conditions must be satisfied before the process can be considered complete?	
Outputs	What data is required to be included in the output? What are the output formats?	Printed reports Distribution (dissemination)

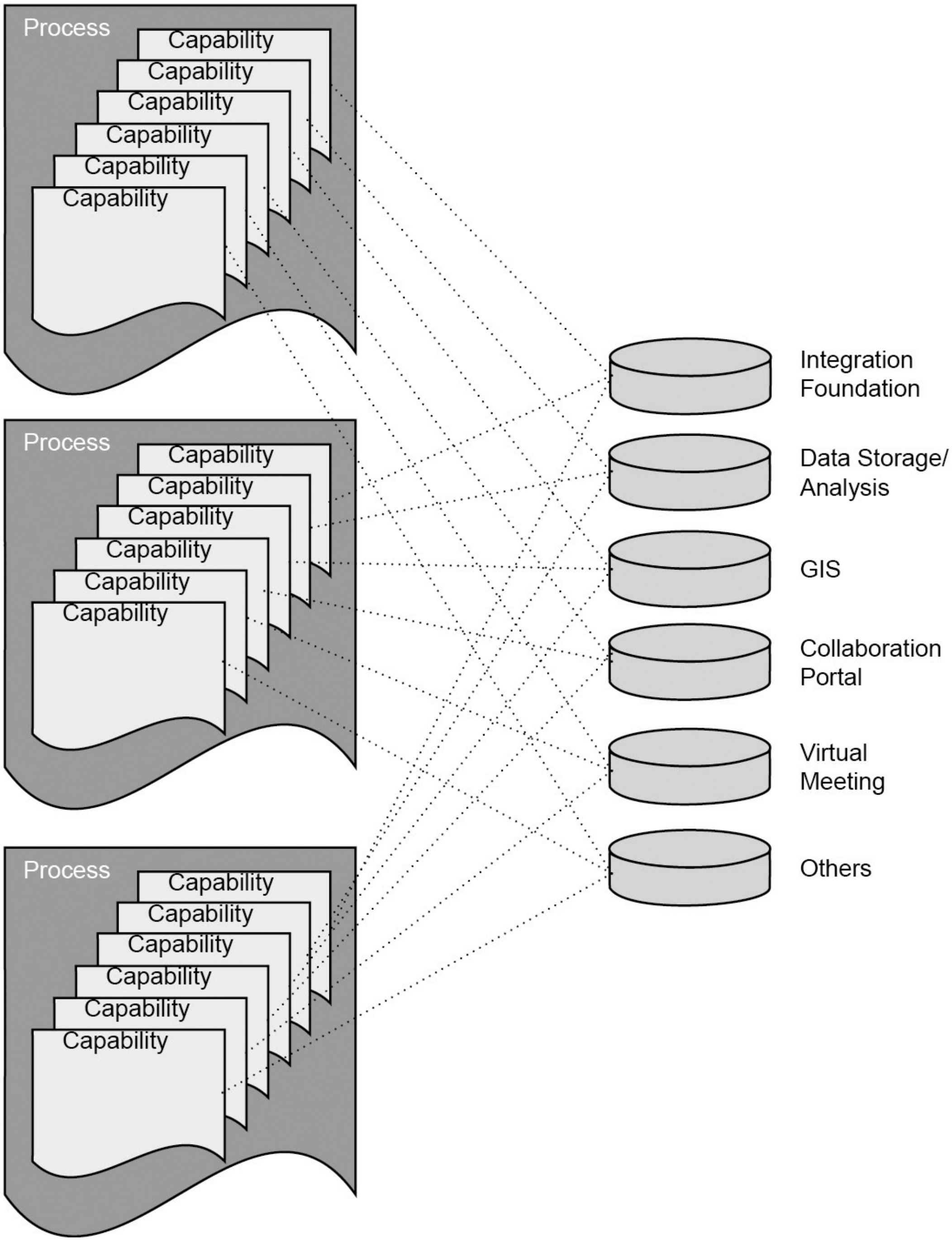
When you finish documenting a process, its capabilities, and its flowchart, you will end up with several documents describing in detail that process.



Each capability can then be connected to a technology/tool of your choice to further define/visualize the process (optional step). This may prove beneficial when choosing technologies for the fusion center.



Then, as a final step, capabilities defined for multiple processes may be linked to technologies to provide the "big picture" and to identify which technologies would be the most beneficial to implement.



Implementation Considerations/ Next Steps

Training

A key ingredient of a successful fusion center implementation is personnel training. Training is important since there are a substantial number of standards and reporting requirements that must be clearly understood for the fusion center to comply with local, state, and federal regulations. The goal of the training is to professionalize and enhance the practice of criminal intelligence within the United States law enforcement/criminal justice community, demonstrate the benefits derived from the intelligence, and encourage information sharing in support of the intelligence.

The International Association of Chiefs of Police (IACP) *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels* included the recommendation to "promote intelligence-led policing through a common understanding of criminal intelligence and its usefulness."[3] The IACP "Core Recommendations to Achieving the Plan" identified several intelligence training issues:

- Training should provide recipients with the skills to provide targeted, evaluative summary data to decision makers.
- Appropriate training must be provided to both current and entering law enforcement personnel on information sharing systems and criminal intelligence concepts.
- Training should promote building trust for intelligence sharing and maintaining civil rights/constitutional protections.
- Training should emphasize that all personnel, regardless of their job, have a role in intelligence and sharing information.
- Training should equip personnel to use new technologies. Standards for training in intelligence functions are critical to implementing a national model for intelligence-led policing. National intelligence training standards can provide criminal justice agencies, individually and collectively, with the framework for achieving that end.

Other examples of training include Information Exchange Sharing using the National Information Exchange Model (NIEM) training as well as the concepts of the Information Sharing Environment (ISE) and the Justice Reference Architecture (JRA).

See Appendix 4: Additional Resources for related resources.

[3] See *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels, Recommendations From the IACP Intelligence Summit*, August 2002, pp. 15 and 16, http://www.cops.usdoj.gov/files/ric/Publications/criminalintelligencesharing_web.pdf.

Technology Assistance

The federal government has provided a number of resources to assist fusion center directors in the development and implementation of core capabilities at their specific fusion centers. One such resource is the provision of a technology assistance engagement. A technology assistance program typically consists of a group of subject-matter experts who provide advice on issues that may be faced by the fusion center director. These engagements are provided by different organizations and, in most cases, are funded by departments such as the Bureau of Justice Assistance (BJA) or the U.S. Department of Homeland Security (DHS).

Numerous technology assistance offerings relevant to fusion centers are provided by the DHS/FEMA Technical Assistance: Preparedness and Program Management program. See Appendix 4.

Requests for technology assistance can be made to the various providers—see Appendix 4: Additional Resources for related resources.

Consultants

Consultants are another resource that can assist fusion center directors in the identification and implementation of core and additional capabilities. Unlike technology assistance programs funded by grantor agencies, fusion centers must directly pay for consulting services. Fusion centers can use consultants to assist with a number of initiatives, such as:

- Creating the specific business architecture documents for the fusion center.
- Selecting the right set of tools and methodologies.
- Creating RFPs.
- Selecting vendors.
- Implementing these capabilities at the fusion centers.

Governance

Defining and implementing a governance structure is one of the key components of planning and implementing a successful fusion center. The governance structure is helpful in guiding the fusion center through the identification, acquisition, and implementation of the core and noncore business capabilities.

As indicated by the National Governors Association (NGA) Center for Best Practices,[4] a well-structured homeland security organization can contribute to a state's ability to prepare for, mitigate, and respond to a range of threats. State homeland security structures, for the most part, did not exist prior to the September 11, 2001, terrorist attacks, and in many cases, they remain a work in progress years after those attacks. However, three guiding principles have emerged that can help Governors determine the appropriate homeland security structure for their states:

- The state homeland security department, office, council, or committee should reflect the Governor's vision, establish the state's security strategy, encompass all necessary stakeholders, and include an all-hazards approach.
- The entity responsible for homeland security should have sufficient budget oversight and authority to allocate funds based on the overarching strategy.
- The Governor should appoint a homeland security director who understands and can manage the diversity of related disciplines, including public safety, the National Guard, and emergency management. The director should also have an understanding of disciplines outside of the department that may impact the security of a state, including public health.

These principles can be leveraged by the fusion centers as they should integrate into the overall Homeland Security Strategy for the state.

Additionally, through the DHS/DOJ Fusion Process Technical Assistance Program, the *Fusion Center Governance Structure and Authority* technical assistance service is also currently available to facilitate the strategic planning for and development of a comprehensive fusion center governance structure, to include legal foundation (statutory authority, executive order, charter/bylaws, and formal partnership agreements) and executive steering committee/subcommittee structure and authorities. See Appendix 4.

[4] *A Governor's Guide to Homeland Security*, by the National Governors Association Center for Best Practices, 2007, p. 19, http://www.nga.org/Files/pdf/0703GOVGUIDEHS.pdf.

Acknowledging That Candidate Technologies Do Support Business Processes

Understanding the business characteristics and corresponding capabilities is the first and most significant step in moving effectively toward implementation of a fusion center. With the understanding gained from the business architecture exercise, a fusion center manager is better equipped to make informed decisions when it becomes necessary to select technologies with product capabilities that map to the business processes. The illustrations below are just a few examples of how candidate technologies can be leveraged to support business processes.

Keep in mind that the purpose of this document is to provide a tool for constructing business architecture; it would not be appropriate for this document to suggest a technical architecture or to recommend specific products. However, technology decisions must ultimately be driven from the overall business needs of the organization. This section outlines some candidate technologies that provide foundation functionality for a wide range of fusion center business processes.

The technology components described in this section are not intended to define a "technical architecture" but rather to offer a starting point for conversations between fusion center managers and their technical service providers, be they agency personnel or contracted personnel.

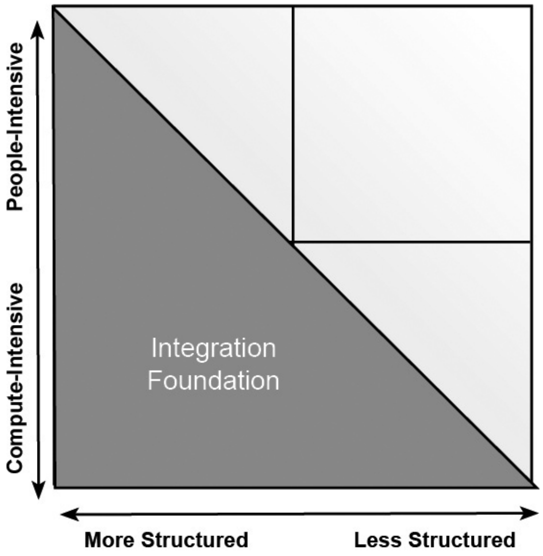


Illustration 3—Integration Foundation

The purpose of this section of the document is to provide business stakeholders with a basic overview that will enable them to:

- Communicate more effectively with their technical counterparts.
- Help determine that technical spending decisions are made in alignment with the business needs of the organization.

If the fusion center aims to deploy a large number of business processes that fall into the "compute-intensive, more structured" category, it may be important to select specific technologies that enable these processes. These technologies may be referred to generically as "integration foundation." The integration foundation provides a general purpose solution for "data in motion," providing a secure, reliable, and scalable means for sharing information across organizational boundaries. For example, if the fusion center requires near real-time feeds of criminal history from outside repositories to an internal analysis repository, an interoperability capability may well be needed. Clearly, an incremental assessment of current capabilities is necessary, but ultimately, in order to deliver on the capabilities set out in this document, the following capabilities will most likely be needed:

- Ability to trigger automated business processes
- Secure movement of data across networks
- Translation of data to/from standard formats
- Auditing and monitoring of business processes
- Alerts and notification to recipients of information

More detailed guidance on how to provide for the capabilities outlined in this section is available in the Justice Reference Architecture (JRA) under development by the Global Infrastructure/Standards Working Group, available at http://it.ojp.gov/globaljra. In reviewing the Global JRA, the reader will be introduced to the full range of issues involved in integration—governance, policy, interface design, standards, and infrastructure. Additionally, a JRA Concept of Operations (CONOPS) document, designed to be valuable to program managers (i.e., a fusion center manager), will explain the why, what, and how (high level) of integration architecture and Service-Oriented Architecture (SOA). The CONOPS principle has certainly already demonstrated value in the integrated justice field, and because of the variations in business needs and the variations depicted by the quadrants shown in Illustration 3 above, the JRA CONOPS will become equally as valuable for fusion centers. It is the complexity of the interoperability foundation driven by the need to meet requirements in neighboring quadrants of the chart that makes this one of the most difficult exercises in determining what technologies are necessary to meet operational expectations. If a fusion center needs only a few business processes in these adjacent quadrants, the interoperability foundation may be extended and customized to serve these needs. However, if the fusion center needs a significant number of business processes in these categories, it may be necessary to investigate the value of other candidate technologies described below.

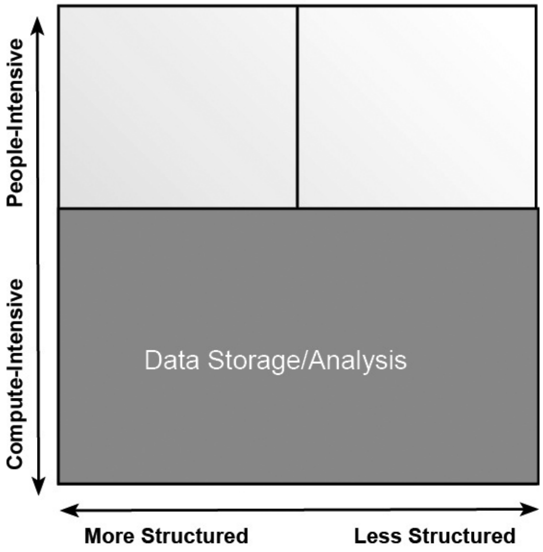


Illustration 4—Data Storage/Analysis

For all types of compute-intensive business processes, data storage/analysis solutions provide an infrastructure for "data at rest." This technology category provides a secure and reliable repository for data.

For "compute-intensive, more structured" processes, transactional database management systems are typically most appropriate. For "compute-intensive, unstructured" processes, data analysis technology provides support for ad hoc data queries and analysis.

As Illustration 5 indicates, Geographic Information Systems (GIS) are an important technology enabler for almost any type of business process that the fusion center needs to perform. For most fusion center stakeholders (police, fire, emergency management, intelligence, etc.), almost all information makes more sense if it is shown on a map. The very nature of fusion center work makes GIS a key capability to consider.

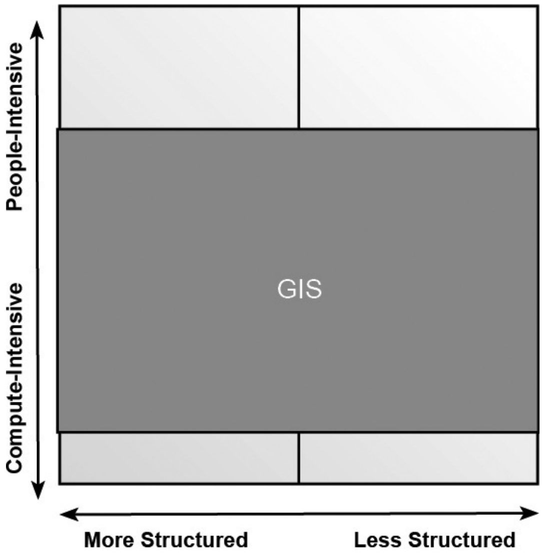


Illustration 5—GIS

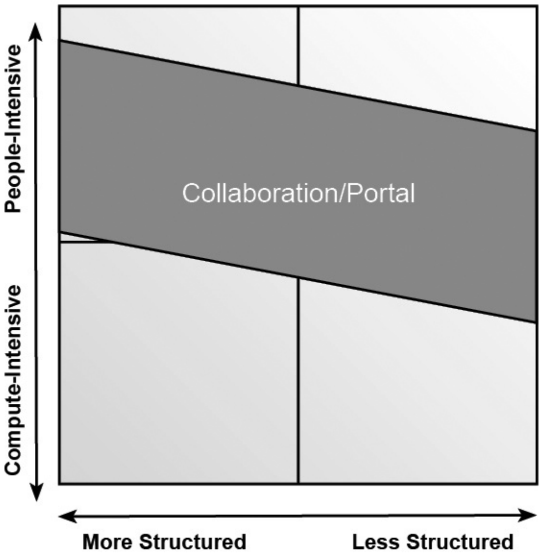


Illustration 6—Collaboration/Portal

Today, some practitioners find that they actually need two types of GIS:

- A "heavyweight" GIS solution that includes state-owned pictometry and can display underground infrastructure layers. These solutions are typically tightly controlled by IT systems administrators. They can show valuable data but are less open to manipulation by power users with ad hoc needs.
- A "lightweight" GIS solution that may contain less detail but is more malleable and accessible to power users who want to experiment with data for ad hoc needs.

As we move into the "people-intensive" quadrants of the diagram, Collaboration/Portal technology becomes a key candidate technology to enable business processes. Functionality provided by these solutions includes:

- Document sharing
- Document libraries
- Threaded discussion
- Project management
- Work group coordination
- Task management
- Workflow management
- Polling and voting

While Collaboration/Portal technology (described above) provides a foundation for most people-intensive processes in the fusion center, it does not cover processes that are less structured. As shown in Illustration 7 Virtual Meeting solutions are appropriate for this type of business process. Functionality provided by Virtual Meeting solutions includes:

- Presence over distance
- Voice and video connectivity
- Shared presentations
- Shared whiteboard
- File and desktop sharing

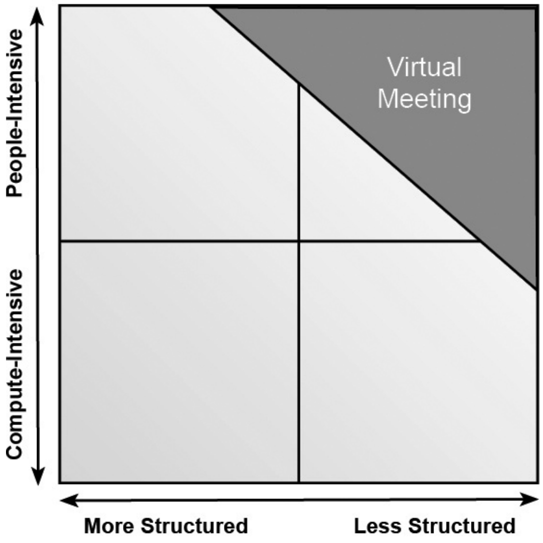


Illustration 7—Virtual Meeting

Appendix 1: Business Process Case Studies

This appendix provides two examples of the final business architecture guidelines for two business processes.

These are examples only and not intended to be "production ready" due to individual variances among fusion center capabilities, styles, missions, resources, priorities, etc.

In addition, these examples are simplified to assist in understanding the concept of business architecture—many more capabilities are expected to be utilized in each process than demonstrated here.

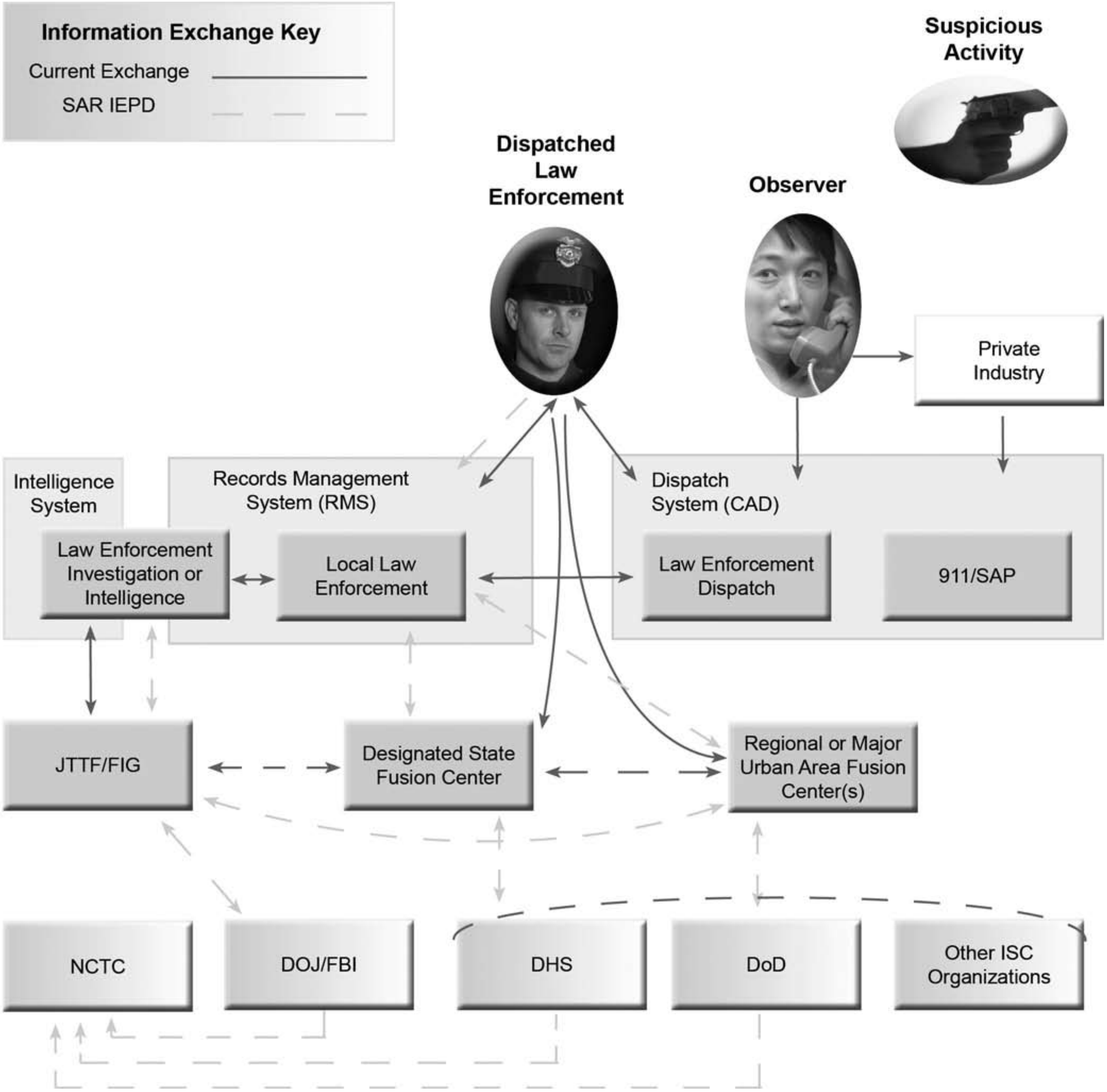
Suspicious Activity Reporting (SAR)

In order to illustrate the business case mapping process, the Suspicious Activity Reporting (SAR) process is used as the first example. The SAR data exchange is designed to support the sharing of suspicious activity, incident, or behavior (hereafter referred to as activity) information throughout the Information Sharing Environment (ISE) and between fusion centers and their law enforcement or intelligence information sharing partners at the local, state, tribal, and federal levels. These SARs will provide for the discovery of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory. Standardized and consistent sharing of suspicious activity information with the state-designated fusion centers is deemed vital to assessing, deterring, preventing, and/or prosecuting those planning terrorist activities.

As a visual aid to the SAR process, below is the data flow diagram from the SAR Information Exchange Package Documentation (IEPD).[5] Note the fusion center entities (designated state fusion center and the regional or major urban area fusion centers) in the center of the diagram.

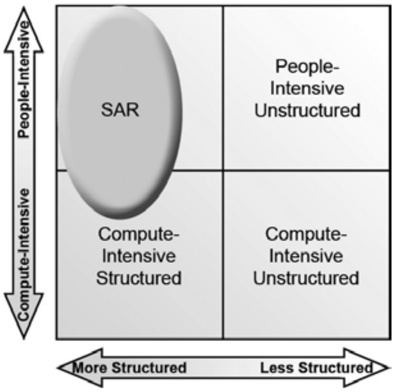
[5] An "Information Exchange Package" represents a set of data that is transmitted for a specific business purpose. It is the actual XML message that delivers the payload or information. (The word "package," as used, refers to a package of the actual data, not a package of artifacts documenting the structure and content of the data.)
An "Information Exchange Package Documentation" (IEPD) is a collection of artifacts that describe the structure and content of an Information Exchange Package. It is used by technologists to assist with their implementation of the exchange.

Figure 1—SAR Information Exchange Flow



Step 1—Describe the Business Process

Using the template, the description of the SAR process looks like this:

Process Description		
Process Name	Suspicious Activity Reporting (SAR)	
Description	SAR is designed to support the sharing of suspicious activity, incident, or behavior (hereafter referred to as activity) information throughout the Information Sharing Environment (ISE) and between fusion centers and their law enforcement or intelligence information sharing partners at the local, state, tribal, and federal levels. The collection, analysis, and exchange of this data assists local, state, tribal, and federal agencies in identifying and responding to both criminal and terrorism activities.	
Rationale	Providing the SAR information into the fusion center network allows for the discovery of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory.	
Benefits	Standardized and consistent sharing of suspicious activity information with the state-designated fusion centers is deemed vital to assessing, deterring, preventing, and/or prosecuting those planning terrorist activities.	
Business Needs	 People-Intensive Compute-Intensive SAR People-Intensive Unstructured Compute-Intensive Structured Compute-Intensive Unstructured More Structured Less Structured Suspicious Activity Reporting is largely dependent on people to collect, report, and analyze the data, so it falls mostly into the People-Intensive section on the vertical scale. In a recent project, the components (down to the individual element level) and data flow of SAR reporting were defined by the Office of the Director of National Intelligence and the U.S. Department of Justice. As a highly structured process, it is placed on the left on the horizontal "Structured" axis. We can now visually represent the SAR business process as a very structured and largely people-driven process.	
Associated Capabilities	• Fusion Process Capability A.1—Intrastate Coordination • Fusion Process Capability A.3—Information Requirements • Fusion Process Capability A.4—Suspicious Activity Reporting (SAR) • Fusion Process Capability A.6—Situational Awareness Reporting • Fusion Process Capability A.9—Coordination With Private Sector and Critical Infrastructure and Key Resources (CIKR) Information Sharing • Fusion Process Capability B.1—Information-Gathering and -Reporting Strategy • Fusion Process Capability C.2—Levels of Confidence • Fusion Process Capability D.1—Analytic Products • Fusion Process Capability D.2—Fusion Process Management • Fusion Process Capability D.4—Information Linking • Fusion Process Capability D.5—Strategic Analysis Services • Fusion Process Capability E.1—Dissemination Plan • Fusion Process Capability E.3—Reporting of Information to Federal Partners • Management and Administrative Capability A.3—Collaborative Environment • Management and Administrative Capability B.3—Privacy Protections • Management and Administrative Capability C.3—Securing Information • Management and Administrative Capability D.3—Training Plan • Management and Administrative Capability E.3—Communications Plan Capabilities included in this example are representative and may not include all capabilities needed to completely document the process.	
Audit	Current Status	SAMPLE
	Creation Date	TBD
	Date Approved/Rejected	TBD
	Reason for Rejection	TBD
	Last Date Reviewed	TBD
	Last Date Updated	TBD
	Reason for Update	TBD

Step 2—Create a Template for Each Associated Baseline Capability

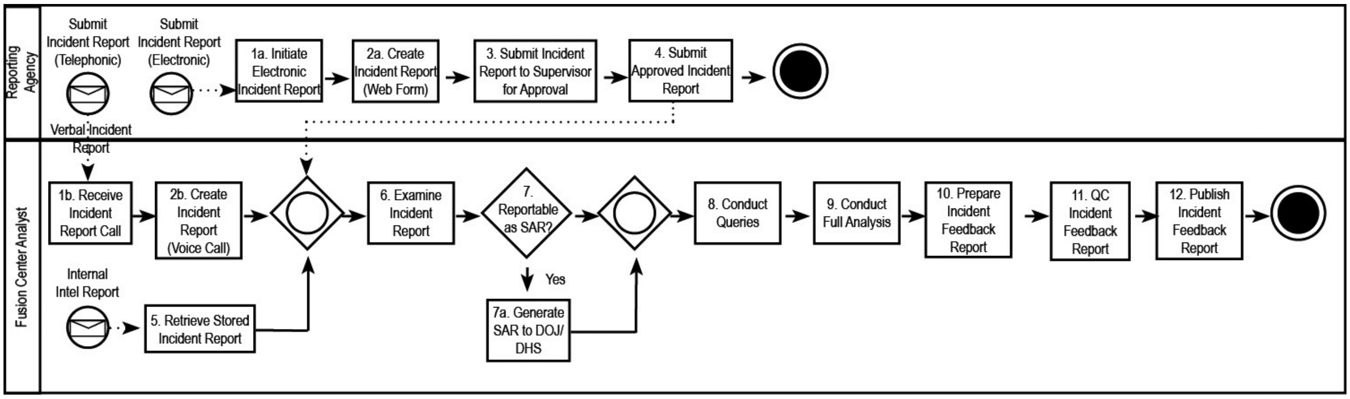
The process calls for each associated capability identified in the previous template to have its own "capability template." An example is provided below.

Capability Description		
Overview	Capability	Management and Administrative Capability A.3—**Collaborative Environment**
	Description	Developing a collaborative environment is essential to the operation of a successful fusion center. Collaboration, as outlined in the Information Sharing Environment (ISE), allows participants not only to share multimedia data and information but to find communities of interest through searches or ISE recommendations based on user activities and behaviors. Collaborative environments can be either enduring, such as the ongoing sharing of information on a particular target or target methodology, or ad hoc, such as mission planning, investigation, or course-of-action development.
	Rationale	Fusion centers embody the core of collaboration. The *Fusion Center Guidelines* define *fusion* as a "*collaborative effort* of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity." As such, collaboration is viewed as essential to *maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.*
	Benefits	Collaboration enables the users to gain access to a wide range of information from a variety of sources, including other governmental and enforcement agencies as well as outside entities. Access to information is critical to the fusion center mission. As demands increase and resources decrease, fusion centers, through collaboration, will become an effective tool to maximize available resources and build trusted relationships.
	Associated Processes	In the interest of developing a collaborative environment, consider the following processes: • Conduct regular meetings with center personnel, and participate in networking groups and organizations. • Educate and liaise with elected officials and community leadership to promote awareness of center operations. • Integrate public and private sector entities into the intelligence function, as appropriate. • Create a representative governance structure. • Utilize MOUs or other types of agency agreements, as appropriate.
	Related Capabilities	• Fusion Process Capability A.7—Data Sources. • Fusion Process Capability A.9—Coordination With Private Sector and Critical Infrastructure and Key Resources (CIKR) Information Sharing. • Fusion Process Capability E.1—Dissemination Plan. • Fusion Process Capability E.2—Reporting of Information to Other Centers. • Fusion Process Capability E.3—Reporting of Information to Federal Partners. *This list of related capabilities is not meant to be all-inclusive. It provides an example of capabilities related to creating a collaborative environment.*
Reference Documents	• *National Strategy for Information Sharing*, http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html. • *Fusion Center Guidelines,* http://it.ojp.gov/documents/fusion_center_guidelines.pdf. • *Information Sharing Environment Implementation Plan,* http://www.ise.gov/docs/reports/ise-impplan-200611.pdf. • National Governors Association Best Practices, http://www.nga.org/portal/site/nga.	
Standards and Governance	While there are no formal standards for collaboration, the organizations below have contributed, either directly or indirectly, to the body of knowledge related to collaboration: • Global Intelligence Working Group (GIWG). • Criminal Intelligence Coordinating Council (CICC). • Global Infrastructure/Standards Working Group (GISWG). • National Association for Justice Information Systems (NAJIS). • National Association of State Chief Information Officers (NASCIO). • Global Advisory Committee (GAC).	

Capability Description		
Stakeholders and Roles	Local Agencies	Homeland security directors—executive oversight to assist in establishing a collaborative environment through executive sponsorship. Regional sharing center (Regional Law Enforcement Exchange [RLEX]-type) managers—manage the effort and drive the process of collaboration, including the establishment of MOUs and the governance structure. Local fusion center directors (where applicable)—manage the effort and ensure compliance. Commanders in charge of intelligence—manage the intelligence function and ensure cooperation and resource deployment. Liaison officers from participating agencies—serve as the primary interface between the agency and other fusion center participants. Law enforcement CIOs and technology directors—primary interface between the IT personnel and other fusion center participants.
	State Agencies	Homeland security directors—executive oversight to assist in establishing a collaborative environment through executive sponsorship. State fusion center directors (where applicable)—manage the effort and ensure compliance. Commanders in charge of intelligence—manage the intelligence function and ensure cooperation and resource deployment. Liaison officers from participating state agencies—serve as the primary interface between the agency and other fusion center participants. State CIOs and technology directors—primary interface between the IT personnel and other fusion center participants.
	Federal Agencies	Homeland security personnel—help to align federal resources with state and local resources. Supervisory agent in charge—ensures adequate participation and cooperation in the exchange of information. Liaison officers from participating federal agencies—serve as the primary interface between the agency and other fusion center participants. Agency CIOs and technology directors.
	Other Fusion Centers	Fusion center directors—work with counterparts to maintain cooperative relationships to ensure the exchange of information. Commanders in charge of intelligence—collaborate with counterparts in other fusion centers. Regional sharing center (RLEX-type) managers—work with fusion center managers to develop collaborative relationships and ensure the exchange of vital information. Law enforcement CIOs and technology directors—primary interface between the IT personnel and other fusion center participants.
	Private Sector	Security managers—liaise with fusion center personnel in the exchange of needed information. Risk management managers—liaise with fusion center personnel in matters related to critical infrastructure protection.
Environmental Trends in Conflict	• Privacy issues often prohibit collaboration and sharing of certain information. • Information security can prohibit collaboration in the sharing of certain information. • Potential disconnect between and among state, local, and federal agencies. • Turf and the control of information. There is a need to address a number of central questions related to control of information: Who owns the data? Who has access to it? How can information be used? Where will it be stored? Resolving these "turf issues" is central to gaining buy-in and collaboration among local agencies and governments.	
Associated Compliance Components	Among the compliance components are the following. Many of these provide either suggestions or best practices associated with fusion and collaboration. • 28 CFR Part 23 • *National Strategy for Information Sharing* • *Fusion Center Guidelines* • *Information Sharing Environment Implementation Plan* • National Governors Association Best Practices	

Capability Description		
Methodologies	• Maintaining a diverse membership to include representatives from local, state, tribal, and federal law enforcement. • Developing and participating in networking groups and organizations that exist locally, regionally, statewide, nationally, and internationally. • Working with Joint Terrorism Task Forces, Anti-Terrorism Advisory Councils, DOJ, DHS, other state and local entities, and other relevant organizations or groups. • Conducting regular meetings for the purpose of collaboration and information sharing. Establishing procedures for maintaining the continuity of personal, organizational, and institutional relationships. • Educating and training the law enforcement community on the intelligence process and fusion center operations. • Educating and liaising with elected officials and other community leaders to promote awareness of the fusion center functions.	
Documentation Requirements	• Mission statement • Goals • MOUs • Governance structure showing participating agencies • Privacy and civil liberties policy	
Associated Technology Areas	• Instant messaging • Secure collaboration portal • Secure e-mail	
Audit	Current Status	SAMPLE
	Chronological Ranking/Priority	TBD
	Creation Date	TBD
	Date Approved/ Rejected	TBD
	Reason for Rejection	TBD
	Last Date Reviewed	TBD
	Last Date Updated	TBD
	Reason for Update	TBD

Step 3—Flowchart the Process

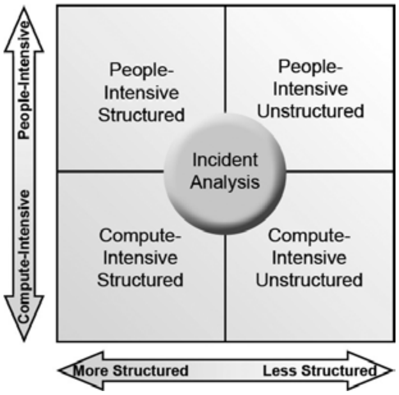

Reporting Agency
Submit Incident Report (Telephonic)
Submit Incident Report (Electronic)
1a. Initiate Electronic Incident Report
2a. Create Incident Report (Web Form)
3. Submit Incident Report to Supervisor for Approval
4. Submit Approved Incident Report
Verbal Incident Report
Fusion Center Analyst
1b. Receive Incident Report Call
2b. Create Incident Report (Voice Call)
6. Examine Incident Report
7. Reportable as SAR?
Yes
7a. Generate SAR to DOJ/ DHS
8. Conduct Queries
9. Conduct Full Analysis
10. Prepare Incident Feedback Report
11. QC Incident Feedback Report
12. Publish Incident Feedback Report
Internal Intel Report
5. Retrieve Stored Incident Report

Law Enforcement Incident Data Collection and Analysis

A second example is the Collection and Analysis of Law Enforcement Incident Data.

Step 1—Describe the Business Process

Using the template, the description of the Law Enforcement Incident Data Collection and Analysis process looks like this:

Process Description		
Process Name	Law Enforcement Incident Data Collection and Analysis	
Description	This is the process of collecting and analyzing law enforcement incident data for (1) investigative purposes (linking cases via modus operandi [MO] and similarities regarding time, distance, offense types, etc.) and (2) anti-terrorism purposes (crimes against high-value targets, victims connected to high-value targets, patterns that when connected may indicate a link to terrorist activity, etc.).	
Rationale	Criminals operate beyond jurisdictional boundaries. The combination of incident data across multiple jurisdictions can frequently yield additional linkages, identification of patterns, combination of similar cases, etc., which in turn greatly assist law enforcement investigative efforts.	
Benefits	The more information available about a crime or a series of related crimes, the greater the likelihood of offender identification, serial crime detection, and offender apprehension.	
Business Needs	 People-Intensive Structured People-Intensive Unstructured Incident Analysis Compute-Intensive Structured Compute-Intensive Unstructured People-Intensive Compute-Intensive More Structured Less Structured Law Enforcement Incident Data Collection and Analysis is largely dependent on people to collect and analyze the data and computer systems to report the data. It also tends to be a somewhat subjective and loosely structured process, left to investigators to spot similarities and trends. Some jurisdictions have software that assists in this analysis. We will visually represent this business process as slightly less structured and a little more people-driven than a computer-driven process.	
Associated Capabilities	- Fusion Process Capability A.1—Intrastate Coordination - Fusion Process Capability A.3—Information Requirements - Fusion Process Capability B.1—Information-Gathering and -Reporting Strategy - Fusion Process Capability D.1—Analytic Products - Fusion Process Capability D.2—Fusion Process Management - Fusion Process Capability D.4—Information Linking - Fusion Process Capability D.5—Strategic Analysis Services - Fusion Process Capability E.1—Dissemination Plan - Management and Administrative Capability B.3—Privacy Protections - Management and Administrative Capability C.3—Securing Information - Management and Administrative Capability D.3—Training Plan - Management and Administrative Capability E.3—Communications Plan Capabilities included in this example are representative and may not include all capabilities needed to completely document the process.	
Audit	Current Status	SAMPLE
	Creation Date	TBD
	Date Approved/Rejected	TBD
	Reason for Rejection	TBD
	Last Date Reviewed	TBD
	Last Date Updated	TBD
	Reason for Update	TBD

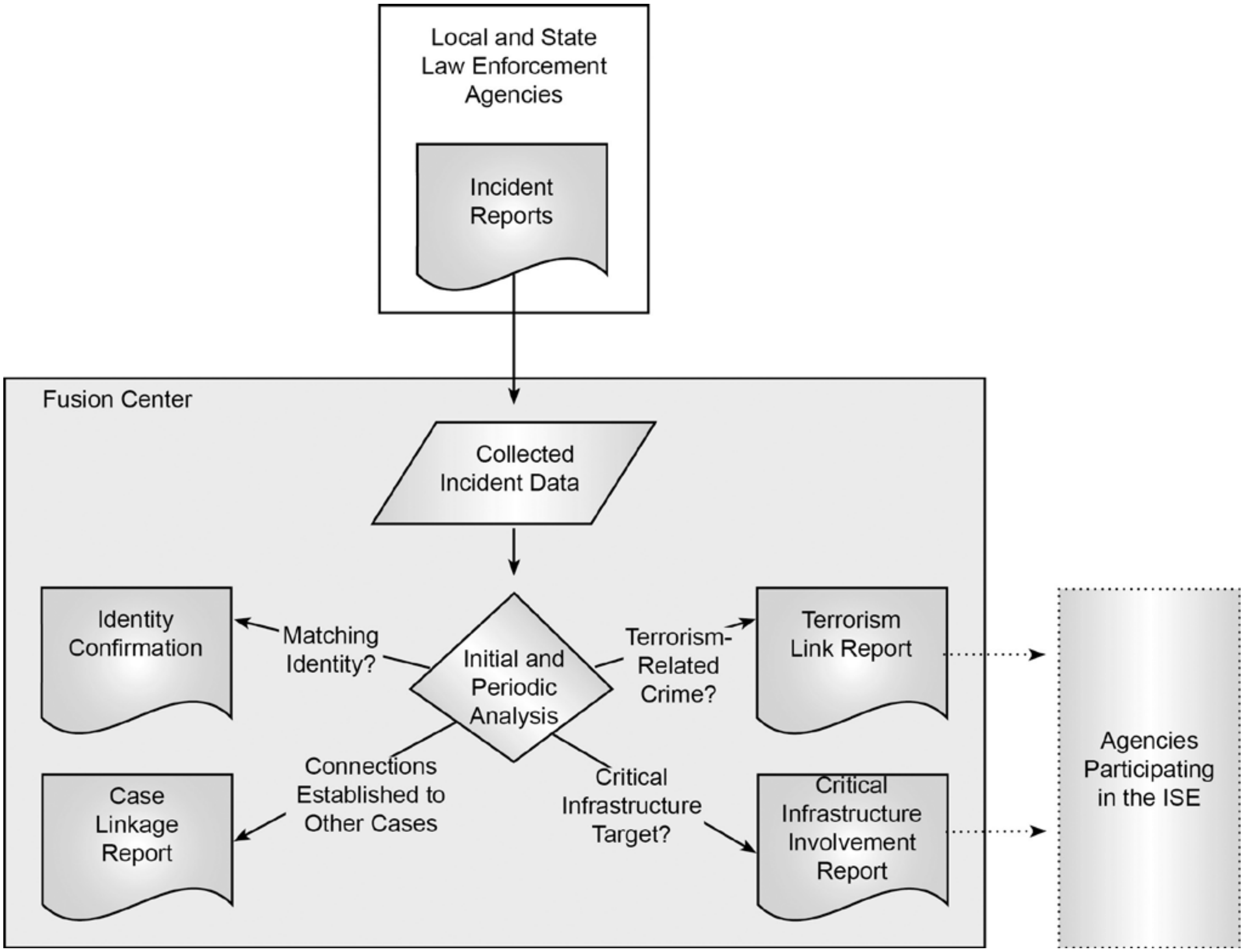
Step 2—Create a Template for Each Associated Baseline Capability

The process calls for each associated capability identified in the previous template to have its own "capability template." An example is provided below.

Capability Description		
Overview	Capability	Fusion Process Capability D.5—**Strategic Analysis Services**
	Description	Fusion centers shall develop the capability to provide strategic analysis services for the jurisdiction served. Fusion centers require a process for reviewing new information and evaluating that new information with historical incidents, events, or activities to identify relationships between criminal activities and/or ongoing investigations.
	Rationale	Criminal activity typically occurs over a period of time and/or disparate geographies. In order to facilitate identification of crime trends, suspects, and activities, fusion center personnel must be able to review, evaluate, and identify relationships within these activities over time and multiple jurisdictions.
	Benefits	Identification of relationships provides for quicker identification of the suspect, activity, and trends. Criminal activity occurring over multiple jurisdictions can be more efficiently investigated, requiring less time and resources.
	Associated Processes	One of the key aspects of this capability is the ability of the analyst to quickly and easily identify, recover, and associate the collected data with new and current events/incidents. Search capabilities across the enterprise, both classified and unclassified, facilitate more comprehensive data, which usually leads to better analysis and conclusions.
	Related Capabilities	• Fusion Process Capability A.1—Intrastate Coordination • Fusion Process Capability A.7—Data Sources • Fusion Process Capability B.3—Collection and Storage of Information • Fusion Process Capability C.1—Information Collation • Fusion Process Capability D.1—Analytic Products • Fusion Process Capability D.2—Fusion Process Management • Fusion Process Capability D.3—Enhancing Analyst Skills • Fusion Process Capability D.4—Information Linking • Fusion Process Capability D.8—Analytical Tools • Fusion Process Capability E.1—Dissemination Plan • Management and Administrative Capability A.3—Collaborative Environment • Management and Administrative Capability B.3—Privacy Protections • Management and Administrative Capability C.3—Securing Information *This list of related capabilities is not meant to be all-inclusive. It provides an example of capabilities related to creating a collaborative environment.*
Reference Documents	• *Fusion Center Guidelines,* http://www.it.ojp.gov • *Information Sharing Environment Enterprise Architecture Framework* (**ISE-EAF**), http://www.ise.gov • *Law Enforcement Analytic Standards,* http://www.it.ojp.gov • *Minimum Criminal Intelligence Training Standards*, http://www.it.ojp.gov/documents/minimum_criminal_intel_training_standards	
Standards and Governance	• LEIU *Criminal Intelligence File Guideliness,* http://www.it.ojp.gov • 28 Code of Federal Regulations (CFR) Part 23 • *Common Terrorism Information Sharing Standards (**CTISS**) Program Manual,* http://www.ise.gov • Information Sharing Environment Privacy Guidelines, http://www.ise.gov	
Stakeholders and Roles	Local Agencies	Local fusion center and regional sharing directors (where applicable)—manage the information exchange process, including data analysis. Commanders in charge of intelligence—manage the intelligence function, develop procedures associated with data analysis, and ensure that analysis includes dynamic crime information. Analysts—implement procedures and use tools to analyze and extract relevant data and align it with incoming crime information. Law enforcement CIOs and technology directors—provide the technology necessary for advanced analysis and integration of sources.

Capability Description		
	State Agencies	Homeland security directors—work with stakeholders to establish protocols for analysis and ensure the inclusion of real-time crime information. State fusion center directors (where applicable)—manage the effort and ensure that protocols are followed and that analysts have the necessary tools to associate crime and terrorist information. Commanders in charge of intelligence—work with analysts to perfect analytic methods and ensure that relevant crime information is accounted for in the analytic process. Analysts—implement procedures and use tools to analyze and extract relevant data. State CIOs and technology directors—provide the technology necessary for advanced analysis.
	Federal Agencies	Homeland security personnel • Work at a national level to fund research into methods and advanced tools to facilitate the analytical process that includes local crime information. • Assist in establishing the federal-level interagency capability to facilitate the fusing validation, deconfliction, and dissemination of terrorism information to state, local, and tribal (SLT) authorities and the private sector. FBI personnel—work with state and local agencies and share information regarding analytic methodology used by federal personnel. Other role-based federal agency personnel (e.g., U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement (ICE), United States Secret Service, United States Coast Guard, Transportation Security Administration)—work with state and local agencies and share information specific to their roles as it relates to crime. Agency CIOs and technology directors—provide the technology necessary for advanced analysis.
	Other Fusion Centers	Fusion center directors • Manage the effort and ensure that protocols are followed to include the linking of real-time crime information. • Share analytic techniques and regional crime information with other fusion centers.
	Private Sector	Security managers and risk management managers—should collaborate with law enforcement officials in identifying crime threats.
Environmental Trends in Conflict	• Insufficient access to timely regional crime information. • Challenges in building a collaborative environment necessary to share real-time crime information.	
Associated Compliance Components	• *Law Enforcement Analytic Standards* • LEIU *Criminal Intelligence File Guidelines*	
Methodologies	• Establish an infrastructure or framework to enable the sharing of critical information. • Establish an analytical process protocol aligned with national standards and guidelines. • Establish and enforce minimum training requirements for all analysts.	
Documentation Requirements	• Analytic protocol • Training requirements	
Associated Technology Areas	• Interoperable infrastructure (enables sharing and more) • Collaboration tools (facilitate alerts and notifications) • Query tools • Geographic Information Systems (GIS) • Advanced automated search tools, such as Web crawling and information discovery • Link analysis • Visual link analysis	
Audit	Current Status	SAMPLE
	Chronological Ranking/Priority	TBD
	Creation Date	TBD
	Date Approved/ Rejected	TBD
	Reason for Rejection	TBD
	Last Date Reviewed	TBD
	Last Date Updated	TBD
	Reason for Update	TBD

Step 3—Flowchart the Process


Local and State Law Enforcement Agencies
Incident Reports
Fusion Center
Collected Incident Data
Initial and Periodic Analysis
Matching Identity?
Identity Confirmation
Terrorism-Related Crime?
Terrorism Link Report
Connections Established to Other Cases
Case Linkage Report
Critical Infrastructure Target?
Critical Infrastructure Involvement Report
Agencies Participating in the ISE

Appendix 2: Glossary

ATAC	Anti-Terrorism Advisory Council
BJA	Bureau of Justice Assistance
BPML	Business Process Modeling Language
CALEA	Commission on Accreditation for Law Enforcement Agencies
CICC	Criminal Intelligence Coordinating Council
CIO	Chief Information Officer
CTISS	Common Terrorism Information Sharing Standards
CTTWG	Counter-Terrorism Training Coordination Working Group
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
EA	Enterprise Architecture
GAC	Global Advisory Committee
GIS	Geographic Information System
GISWG	Global Infrastructure/Standards Working Group
GIWG	Global Intelligence Working Group
GJXDM	Global Justice XML Data Model
IACP	International Association of Chiefs of Police
IADLEST	International Association of Directors of Law Enforcement Standards and Training
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
IIR	Institute for Intergovernmental Research
IJIS	IJIS Institute
ISE	Information Sharing Environment
ISE-EAF	*Information Sharing Environment Enterprise Architecture Framework*
ISE-IP	*Information Sharing Environment Implementation Plan*
JRA	Justice Reference Architecture
JTTF	Joint Terrorism Task Force
LEIU	Law Enforcement Intelligence Unit
MOU	Memorandum of Understanding
NCISP	*National Criminal Intelligence Sharing Plan*
NCSC	National Center for State Courts
NGA	National Governors Association
NIEM	National Information Exchange Model
PM-ISE	Program Manager, Information Sharing Environment
SAR	Suspicious Activity Report or Suspicious Activity Reporting
SEARCH	The National Consortium for Justice Information and Statistics
SIR	Suspicious Incident Report (replaced by SAR)

SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
UASI	Urban Areas Security Initiative
UML	Unified Modeling Language

Appendix 3: Participants

The creation of this document was a volunteer effort by numerous contributors, and sincere thanks are extended to them for their hard work, time, and persistence.

Special recognition goes to Gerry Wethington, Thomas O'Reilly, the IJIS Institute, the Institute for Intergovernmental Research (IIR), SEARCH, and the National Center for State Courts (NCSC).

Document Contributors

Gerry Wethington (Chair)	Unisys
Scott Came	SEARCH—The National Consortium for Justice Information and Statistics
Lorraine Cimino	Apogen Technologies
Robert Cummings	Institute for Intergovernmental Research
Chuck Dodson	Oracle Corporation
Scott Fairholm	National Center for State Courts
Kael Goodman	GovCore Solutions
Bill Kellett	Microsoft
Scott Parker	IJIS Institute
Sam Ali	IJIS Institute
Philip Ramer	Institute for Intergovernmental Research
Sharad Rao	Tetrus Consulting
Karma Temple	SRA International
Robert Wolf	Convergence
Martin Zaworski, Ph.D.	Unisys
Chuck Georgo	NOWHERETOHIDE.ORG
Michael Dillon	MetroView Consulting, LLC

Advisors and Support Contributors

Ken Clark	Scitor Corporation/Program Manager, Information Sharing Environment (PM-ISE), ODNI
Major Daniel Cooney	New York State Police, Criminal Intelligence Section
Scott Dutton	Georgia Bureau of Investigation, Investigative Division, Georgia Information and Analysis Center
Lieutenant Robert Fox	Los Angeles Police Department, Los Angeles Joint Regional Intelligence Center
Aaron Kustermann	Illinois State Police, Division of Operations, Statewide Terrorism Intelligence Center
Patrick McCreary	Bureau of Justice Assistance (BJA), USDOJ

Tom O’Reilly	Bureau of Justice Assistance (BJA), USDOJ
Russ Porter	Iowa Department of Public Safety, Iowa Intelligence Fusion Center
Kevin Saupp	National Preparedness Directorate, DHS
Paul Wormeli	IJIS Institute

Appendix 4: Additional Resources

DHS/FEMA Technical Assistance: Preparedness and Program Management, Technical Assistance Catalog

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), National Preparedness Directorate (NPD), Technical Assistance (TA) program seeks to build and sustain capabilities through specific services and analytical capacities across two primary functional areas:

Preparedness Technical Assistance services seek to build and sustain capabilities in support of the four homeland security mission areas (prevention, protection, response, and recovery) and the suite of priorities and capabilities outlined in the *National Preparedness Guidelines*. As capability gaps are identified within state and local jurisdictions, Preparedness TA services are designed, developed, and delivered to address those needs and build capabilities in the most critical areas. The following text provides an overview of the services that make up the NPD's Preparedness TA program:

- Prevention Technical Assistance: The prevention mission area focuses primarily on the following two national priorities: (1) Expand Regional Collaboration and (2) Strengthen Information Sharing and Collaboration Capabilities. In coordination with lead federal law enforcement and intelligence agencies (including the DHS Office of Intelligence and Analysis, the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence [ODNI]), NPD seeks to ensure that state and local jurisdictions possess required capabilities and are proficient in tasks essential to preventing terrorist attacks against the homeland. In the prevention mission area, NPD has made the establishment of the fusion capacity the top prevention priority for state and local governments.
- To facilitate the development of a national fusion center capability, the DHS NPD and the U.S. Department of Justice's (DOJ) Bureau of Justice Assistance (BJA) have partnered to develop the Fusion Process Technical Assistance Program. This program includes 11 targeted Fusion Process Technical Assistance Services. Each service supports the implementation of the Global *Fusion Center Guidelines* and the ODNI *Information Sharing Environment Implementation Plan* to facilitate the nationwide development and/or enhancement of the fusion process. Additional information on the joint DHS/DOJ program and these services is located at http://www.ojp.usdoj.gov/odp/docs/info231_Fusion_Process.pdf.
- Protection Technical Assistance: The protection mission area focuses primarily on the following national priorities: (1) Expand Regional

Collaboration; (2) Implement the *National Infrastructure Protection Plan* (NIPP); and (3) Strengthen Chemical, Biological, Radiological, Nuclear, and Explosive Detection, Response, and Decontamination Capabilities. NPD has partnered with the DHS Office of Infrastructure Protection (IP) to enhance protection-related support to state and local jurisdictions.

- Response/Recovery Technical Assistance: The response and recovery mission areas focus primarily on the following four national priorities: (1) Implement the National Incident Management System (NIMS) and National Response Plan; (2) Expand Regional Collaboration; (3) Strengthen Interoperable Communications Capabilities; and (4) Strengthen Chemical, Biological, Radiological, Nuclear, and Explosive Detection, Response, and Decontamination Capabilities. NPD has partnered with the NIMS Integration Center (NIC), the U.S. Department of Energy (DOE), and others to enhance response and recovery-related support to state and local jurisdictions.

Program Management Technical Assistance services provide direct assistance in the establishment and enhancement of the overall homeland security administrative framework within state and local jurisdictions. These technical assistance services help build the infrastructure at the state and local levels in which preparedness purchases, training activities, exercises, and additional assistance can accurately be managed, administered, tracked, and measured. This component of the overall TA program includes services focused on grant reporting, grants management, overall homeland security program management, and resource management strategies for special needs jurisdictions.

For more information—http://www.ojp.usdoj.gov/odp/docs/NPD_Technical_Assistance_Catalog.pdf

IJIS Institute

The IJIS Institute is a 501(c)(3) organization whose mission is to contribute to the successful implementation of integrated justice information systems nationwide by promoting the expertise, knowledge, and experience of the information technology (IT) industry in a way that benefits both the private and public sectors. The IJIS Institute provides this type of assistance to public sector agencies by:

- Delivering training and education to state and local governments on key technology issues and related planning and implementation issues, such as best practices in project management.
- Providing technology assistance to state and local governments to assist in the planning and implementation of integrated justice information systems.
- Participating on boards and committees working to advance the field of justice system information integration, such as standards working groups.
- Actively representing the IT industry's perspective on justice information sharing issues at key stakeholder conferences and meetings.
- Developing relationships and collaborating with key public sector and nonprofit associations in improving information sharing.
- Undertaking research, evaluation, and demonstration projects that benefit the administration of justice.

Education and Training—A central mission of the IJIS Institute is to leverage the expertise of the information technology community by providing training to public sector agencies and industry representatives that is essential to the successful implementation of information sharing projects in the justice and public safety community. IJIS Institute Technology Training provides in-depth education on key information sharing technologies, such as XML and the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM). The IJIS Institute has two primary training delivery models. The first model brings the course to the students, where instructors travel to the requesting agencies in order to minimize the burden associated with student travel. The second model delivers training on the campus of the IJIS Institute Headquarters located in northern Virginia. Course offerings fall into two categories—standard and custom. Standard courses are fully developed for general use and are ready to deliver at any time. Custom courses are developed from scratch or tailor existing course content to meet the unique objectives of each requesting agency.

Technology Assistance—Under a grant awarded by the U.S. Department of Justice, Bureau of Justice Assistance (BJA), the IJIS Institute provides technology assistance to state and local jurisdictions that are implementing integrated justice systems. The goal of the grant is to leverage the expertise and experience of private sector information technology firms in providing timely, objective, and cost-effective technology suggestions and guidance to decision makers, IT project managers, governing bodies, and others faced with technology-related decisions and their implementation. Technology assistance offered by the IJIS Institute under the provisions of the BJA grant provides the following services:

- Limited, short-term engagements (between 1 to 5 days).
- Telephone support for specific technology problem solving.
- Assistance that is staffed by representatives from multiple firms, to ensure a company-neutral assessment.
- Assistance that is focused on technology-related issues and integrated justice system implementation.
- Documentation for the jurisdiction describing the technology assistance and any outcomes. All technology assistance activities will result in the documentation of the technology assistance that will be circulated to the Justice Department, the jurisdiction, and to the IJIS Institute membership. Information about IJIS Institute technology assistance that has national implications for justice information integration will be posted to the IJIS Web site for members and other interested parties.
- Assistance that is structured in a fair and balanced manner, so that firms of the individual IJIS Institute members are not precluded from bidding on subsequent work with the jurisdiction.

Contact information—http://www.ijis.org or (703) 726-3697

Institute for Intergovernmental Research® (IIR)

The Institute for Intergovernmental Research (IIR), a nonprofit research and training organization, specializes in law enforcement, juvenile justice, criminal justice, and homeland security issues. Its offerings include:

Research and Education—IIR provides comprehensive research and education services to a broad range of functions in the public safety domain and also provides assistance to the private sector. The areas of special competence of IIR include management and organization, operations, information systems, planning, research, technical assistance, program evaluation, curriculum development, training, policy development, and implementation. IIR specializes in research and education services involving intergovernmental issues—local, state, tribal, and federal—in the areas of law enforcement, criminal justice, homeland security, and juvenile justice, with concentration in law enforcement agency organization and management, youth gang research, grants management, economic crime, organized crime intelligence, homeland security, and major criminal conspiracy investigations and prosecutions.

Program Evaluation—The program evaluation work of IIR has constituted an important portion of its operations to date. These efforts have included local, multijurisdictional, and nationwide program evaluation activities based on comprehensive research designs and guides. Extensive data collection efforts and detailed descriptive case studies have been key ingredients of IIR's program evaluations. Each evaluation is thoroughly planned through detailed background information compilation, review of program characteristics, design of research questions, establishment of evaluation objectives, and extensive methodological consideration. Products, task plans, and site visits are all specifically scheduled and monitored according to a detailed evaluation management plan.

Policy Analysis and Technical Training—Major policy analysis efforts have been designed and conducted by IIR, primarily at the multistate and national levels. Thoroughly prepared research designs are an integral part of IIR's analysis activities. The research has included the use of literature reviews, mail surveys, personal interviews, data collection through standardized instruments and through on-site collection, and data analysis and presentation, including the use of computerized statistical analytical programs. IIR has also provided technical training to hundreds of agencies throughout the United States and has been funded by the federal government to deliver major technical training services nationwide to federally funded program efforts.

General Training Workshops and Seminars— IIR develops and conducts customized training workshops and seminars for personnel of federal, state, tribal, and local governmental agencies to improve leadership, technical, and managerial skills. Programs have been delivered throughout the United States in the following topic areas:

- Criminal Justice Information Systems, including Criminal Intelligence Systems Operating Policies

- Intelligence Analysis
- Investigative Management
- Narcotics Task Forces
- Methamphetamine Investigations
- Narcotics Control and Organized Crime
- Financial Investigations
- Violent Crime Response
- Grants Management and Programmatic Training

Contact information—http://www.iir.com or (850) 385-0600

National Center for State Courts (NCSC)

The National Center for State Courts, headquartered in Williamsburg, Virginia, is a nonprofit court reform organization dedicated to improving the administration of justice by providing leadership and service to state and local courts.

Founded in 1971 by then U.S. Chief Justice Warren E. Burger and the Conference of Chief Justices, the Center provides education, training, technical assistance, and management and research services to the justice system.

As the country's premier resource for courts, NCSC:

- Serves as a **national think tank** to conduct research, promote experimentation, establish performance standards and measures, identify best practices, and evaluate program performance.
- Provides a **national forum** for discussion of ideas affecting the administration of justice.
- Creates a **national leadership agenda** for improving the administration of justice.
- Provides a **national voice** for the needs and interests of the state courts.
- Promotes **collaboration among national court associations** and related national organizations.
- Serves as an **agent of change** to anticipate new developments and foster adaptation to new circumstances.
- Facilitates and supports the **provision of independent, accessible, responsive forums** for the just resolution of disputes.
- Strengthens the **rule of law** and administration of justice throughout the world.

NCSC's multidisciplinary staff members work in concert to ensure that courts are provided with the most current and relevant information and assistance possible.

Using technology to improve access to justice and increase the efficiency and effectiveness of court operations is one of the Center's core practice areas. Technology can be a powerful tool in our nation's courts; however, identifying and implementing new technology systems can be a daunting and confusing task for administrators, judges, and staff. That is why NCSC proactively works with court systems across the country to evaluate and address their current and future technology needs.

In addition to providing technology policy leadership to courts across the country, NCSC's Technology Division serves as support staff for the Joint Technology Committee—the court community's forum to develop and promote technology standards for the courts and to address concerns about information sharing policies.

NCSC staff members hold key leadership roles on a number of committees that support national justice information sharing, including the Global Advisory Committee, Global Infrastructure/Standards Working Group, National Information Exchange Model (NIEM) Technical Architecture Committee, and NIEM Business Architecture Committee.

For more information—http://www.ncsconline.org/

SEARCH—The National Consortium for Justice Information and Statistics

SEARCH—The National Consortium for Justice Information and Statistics is a nonprofit membership organization created by and for the states. Since 1969, SEARCH's primary objective has been to identify and help solve the information management problems of state and local justice agencies confronted with the need to exchange information with other local agencies, state agencies, agencies in other states, or the federal government.

Technical Assistance Program—SEARCH offers technical assistance to local and state justice agencies in the development, management, improvement, acquisition, and integration of their automated information systems. SEARCH not only works with individual justice agencies (such as a police department implementing a new records management system or a court in the acquisition of a new case management system) but also works with multidisciplinary groups of justice agencies to assist them in planning for and integrating their information systems at local, state, and regional levels. For more than 20 years, SEARCH technical assistance programs have provided both on-site and in-house, no-cost technical assistance to justice agencies throughout the country.

High-Tech Crime Training—SEARCH offers training courses designed to teach high-tech investigators the skills they need to stay ahead of criminals in the fight against crime. Officers new to Internet and computer forensic investigations, as well as advanced digital media investigators, will benefit from the leading-edge curriculum.

Justice Information Exchange Model (JIEM) Tool—This project, funded by the Bureau of Justice Assistance, U.S. Department of Justice, is designed to facilitate the development of integrated justice information systems planning and implementation throughout the nation. Integration of justice information systems refers to the justice community's ability to access and share critical information at key decision points throughout the justice process. The JIEM Modeling Tool is an easy-to-use Web-based software package that enables justice system practitioners to build a model of their "as-is" and "to-be" information exchanges.

JIEM Training—The classes are geared primarily at public sector individuals; sites seeking to use the JIEM Modeling Tool may send representatives to receive in-depth instruction on the JIEM conceptual framework and Web-based modeling tool.

Contact information—http://www.search.org or (916) 392-2550

Global Justice Information Sharing Initiative (Global)

The Global Initiative is a collaborative effort among government bodies and nonprofit organizations to develop and implement a standards-based electronic information exchange capability, providing the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

- Workshop #1—Capability Modeling Report: This is a report based on a workshop that modeled fusion center capabilities as outlined in The *Global Justice Reference Architecture (JRA) Guidelines for Identifying and Designing Services* [JRA-GIS] document. The modeling was performed to identify those capabilities that could provide fusion center "Reference Services" in a Service-Oriented Architecture (SOA).

For more information—http://www.iir.com/global/

Regional Information Sharing Systems® (RISS)

The six RISS Centers provide services to more than 8,200 local, state, tribal, and federal law enforcement agencies. By providing rapid access to information otherwise unavailable or too time-consuming to obtain, the RISS network (RISSNET™) has made a significant difference in the fight against crime.

For more information—http://www.riss.net

National Criminal Intelligence Resource Center (NCIRC)

The NCIRC Web site, http://www.ncirc.gov, serves as a "one-stop shop" for local, state, tribal, and federal law enforcement communities to keep up with the latest developments in the field of criminal intelligence.

The U.S. Department of Justice and the U.S. Department of Homeland Security have made information regarding the Fusion Process Technical Assistance Program and Services available on the National Criminal Intelligence Resource Center (NCIRC) Web site in order to deliver the information to the users in the field. NCIRC is a secure Web site developed to serve as a "one-stop shop" for local, state, tribal, and federal law enforcement agencies to keep up with the latest developments in the field of criminal intelligence. The NCIRC contains a list of services that support and facilitate the implementation of the *Fusion Center Guidelines* and the nationwide development and enhancement of the fusion process. NCIRC also provides a mechanism for requesting additional information about the services, which include:

Fusion Center Services

- **Fusion Process Orientation**: Provides an overview of the fusion process and facilitates the development of a strategic fusion process/center development plan.

- **Fusion Center Governance Structure and Authority**: Assists in the development of a comprehensive governance structure, including legal foundation, steering committee, and subcommittee structure.
- **Fusion Center Concept of Operations (CONOPS) Development**: Organizes the development of the core document used to synchronize current operations and plan future operations.
- **Fusion Center Privacy Policy Development**: Enables the development of an effective privacy policy to ensure that constitutional rights, civil liberties, and civil rights are protected while allowing the fusion center to achieve its mission objectives.
- **28 CFR Part 23 Technical Assistance**: Assists law enforcement agencies in the operation of criminal intelligence systems that comply with the 28 Code of Federal Regulations Part 23.
- **Fusion Center Administration and Management**: Supports the design of a strategic framework to structure the management of personnel and organize assets provided by participating entities.
- **Fusion Liaison Officer Program Development**: Institutionalizes multidisciplinary fusion center participation via the replication of the Fusion Liaison Officer Program.

Information Sharing and Intelligence Services

- **State and Local Anti-Terrorism Training**: Provides specialized awareness orientation regarding terrorism interdiction, investigation, and prevention for law enforcement executives, command personnel, intelligence officers, investigators, analytical personnel, training directors, and prosecutors.
- **Criminal Intelligence for the Chief Executive**: Provides an overview regarding the importance of and responsibilities associated with developing intelligence capabilities within law enforcement agencies.
- **National Information Exchange Model (NIEM) Training**: Provides information regarding the development and implementation of NIEM.
- **Global Justice XML Data Model (GJXDM) Training**: Provides information and resources regarding the development and implementation of GJXDM.

NCIRC is securely accessible via the Regional Information Sharing Systems (RISS) network (RISSNET) and the FBI's Law Enforcement Online (LEO) secure law enforcement Web site. After logging on to either system, enter the URL http://www.ncirc.gov. Additional information about NCIRC and available fusion process services is available via e-mail, information@ncirc.gov, or by calling the NCIRC Program Manager at (850) 385-0600, extension 237.

Lessons Learned Information Sharing (LLIS)

Lessons Learned Information Sharing is the national network of Lessons Learned and Best Practices for emergency response providers and homeland security officials. LLIS's secure, restricted-access information is designed to facilitate efforts to prevent, prepare for, and respond to acts of terrorism and other incidents across all disciplines and communities throughout the United States. (http://www.llis.gov).

The Fusion Process Resource Center (Resource Center), located on http://www.llis.gov, is a secure and restricted database for fusion process-related documents, such as best practices, samples, and templates. The Resource Center is available to appropriate state and local homeland security personnel who are responsible for the development, implementation, and/or operation of fusion centers. The Resource Center consists of the following components:

1. Document and Resource Library, including a repository of documentation (samples, templates, white papers, good stories, etc.) that provides insight into the establishment and operation of fusion centers. Major federal guidelines, grant information, and relevant http://www.llis.gov content are also available via the library.
2. Fusion Center Registry

The LLIS Fusion Process Resource Center has also supported the identification and documentation of several fusion center best practices, including:

- Fusion Center Tools: Arizona Counter Terrorism Information Center's (AcTIC) Facial Recognition Database
- Fusion Center Tools: Ohio Homeland Security's Contact and Information Management System
- Fusion Center Collaboration: State of Washington Joint Analytical Center's Private Sector Integration

- Fusion Center Collaboration: State of Washington Joint Analytical Center—FBI Field Investigative Group Partnership
- Fusion Center Collaboration: Kansas City Regional Terrorism Early Warning Group, Interagency Analysis Center's Data Sharing Agreements
- Fusion Center Case Study: Southern Nevada Counter-Terrorism Center—Supporting Special Events: 2007 NBA All-Star Game
- Fusion Center Case Study: New York State Intelligence Center
- Fusion Center Case Study: AcTIC

These best-practice documents are all posted within the Fusion Process Resource Center on http://www.llis.gov.

Bureau of Justice Assistance
U.S. Department of Justice

For More Information

Please call (850) 385-0600 or e-mail it@it.ojp.gov.
For more information about DOJ information sharing initiatives, go to

www.it.ojp.gov

Issued 04/09