Global Justice Information Sharing Initiative

United States
Department of Justice

Fusion Center Technology Guide

DHS/DOJ Fusion Process Technical Assistance Program and Services

April 2009

Fusion Center Technology Guide

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, the SMART Office, 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

1. Purpose

Fusion centers provide essential contributions towards protecting our communities by providing timely, accurate, and actionable information. This information enables public safety and government leaders to make sound management decisions regarding emerging threats and direct resources to areas of greatest need. Fusion centers also play a critical role in supporting uniformed officers as well as investigators by supporting law enforcement's needs to submit and receive information so they can more effectively and efficiently carry out their duties and responsibilities. Fusion centers are best-equipped to meet tomorrow's challenges when technology is leveraged to foster advances in prevention and investigative tactics. Aligning improved business practices with appropriate technical solutions, technology enables and supports stronger multiagency cooperation by providing secure avenues for justice information sharing. In an era in which criminals and terrorists are known to use technology and engage in criminal enterprises across geographic boundaries, it is critical that fusion centers develop and implement the required policies, practices, and technology solutions to help protect communities while ensuring that the privacy and civil liberties of individuals are also protected.

The purpose of this document is to provide a methodology for fusion center directors and managers to facilitate technology planning and to provide a practical perspective on the value of technology as an enabler to the fusion center mission. This document has been developed to work in conjunction with other fusion center technology information resources.

The general purpose of the fusion center is to provide an aggregation, analysis, and dissemination point for classified and unclassified data relevant to "all-crimes" and "all-hazards" intelligence approaches. In this regard, technology plays an important role in advancing the ability to share this information among a variety of partners across the public and private sectors.

Fusion centers are now in various stages of operation in most states and major urban areas. Many of these centers are still in the early stages of technology implementation. The value of technology quickly becomes apparent when focusing on the challenges and hurdles to information sharing. From defining the common data standards to facilitate common understandings and interpretations of information, to protecting privacy rights through electronic management and enforcement of access controls and retention policies—adequate technology planning and utilization can be a critical enabler to sharing information responsibly and fostering safer communities. Fusion centers that are able to adopt appropriate technologies and standards to meet their business objectives will be better-prepared to handle the challenges today and in the future.

2. Approach

As fusion center operations continue to mature, the adoption of a proven methodology for the selection, acquisition, and implementation of technology solutions is highly recommended. First, it is imperative that a fusion center's technology strategy recognize the principle that technology supports business operations and not vice versa. It is important that a clear understanding of the fusion center mission, goals, critical success factors, and the business processes and functions required to achieve them be established before a supporting technology strategy is developed and implemented.

To effectively develop and execute a technology strategy and implementation plan and to ensure its responsiveness to the broader mission of the fusion center, it is imperative to begin with an assessment of the core capabilities and business functions/processes of the center. This will enable the fusion center to build a business architecture framework that can be used to guide the development of business-driven technology needs. To assist the fusion center in the development of these components, two important documents can be utilized to provide guidance: (1) *Baseline Capabilities for State and Major Urban Area Fusion Centers* and (2) *Defining Fusion Center Business Processes: A Tool for Planning*. Technology-relevant excerpts from each are outlined below.

Baseline Capabilities for
State and
Major Urban Area
Fusion Centers

A Supplement to the
Fusion Center Guidelines

September 2008

Document 1: Baseline Capabilities for State and Major Urban Area Fusion Centers

Specific capabilities that relate to technology functions have been extracted for reference and are presented in the outline below. To review the document in its entirety, please visit the Justice Information Sharing Web site at www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

> *Information systems contribute to every aspect of homeland security. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Databases used for federal law enforcement, immigration, intelligence, public health, surveillance, and emergency management have not been connected in a way that allows us to comprehend where information gaps and redundancies exist. We must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.*
>
> —The *National Strategy for Homeland Security*, July 2002

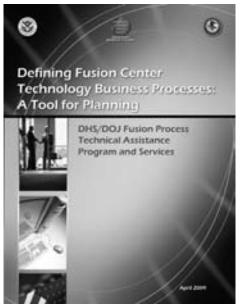
✪ **Fusion Process Capabilities** (BC Section I)

- Planning and Requirements Development (#I.A)
    - ◇ 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. (#I.A.7)
- Information Gathering/Collection and Recognition of Indicators and Warnings (#I.B)
    - ◇ 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. (#I.B.3)
- Processing and Collation of Information (#I.C)
    - ◇ 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. (#I.C.1)
    - ◇ Levels of Confidence—Fusion centers shall liaise with partners to ensure that information collected is relevant, valid, and reliable. (#I.C.2)
- Intelligence Analysis and Production (#I.D)
    - ◇ Analytical Tools—Fusion centers shall provide the necessary tools to analysts for the analysis of information and data. (#I.D.8)

✪ **Management and Administrative Capabilities** (BC Section II)

- Information Technology/Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure (#II.E)
    - ◇ 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. (#II.E.1)
    - ◇ 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. (#II.E.2)
    - ◇ Communications Plan—Fusion centers shall have a plan to ensure safe, secure, and reliable communications, including policies and audit capabilities. (#II.E.3)
    - ◇ Contingency and Continuity-of-Operations Plans—Fusion centers shall have contingency and continuity-of-operations plans to ensure sustained execution of mission-critical processes and information technology systems during an event that causes these systems to fail and, if necessary, to ensure performance of essential functions at an alternate location during an emergency. (#II.E.4)

Document 2: Defining Fusion Center Technology Business Processes: A Tool for Planning


Defining Fusion Center Technology Business Processes: A Tool for Planning
DHS/DOJ Fusion Process Technical Assistance Program and Services
April 2009

This document provides a framework for documenting fusion center business processes and capabilities and mapping them to technology requirements. Use this resource to leverage a useful framework and document templates for describing business processes. To review the document in its entirety, please visit the Justice Information Sharing Web site at http://www.it.ojp.gov/Defining_Fusion_Center_Technology.pdf.

✪ **Core Capabilities** (Chapter 3)

The core capabilities referenced in this section are derived from a variety of sources, including the *National Strategy for Information Sharing*, the *Fusion Center Guidelines,* the *Target Capabilities List,* and the *National Criminal Intelligence Sharing Plan*. The core capabilities listed in this document are to work in tandem with those defined in the *Baseline Capabilities for State and Major Urban Area Fusion Centers* outlined above.

Relevant subsections include:

- Fusion Center Process Capabilities
  This section outlines the considerations for implementing technology capabilities in the fusion center based upon the fusion center mission leveraging national programs, standards, and guidelines (e.g., Suspicious Activity Reporting [SAR]). Technology issues addressed in this section include

planning and requirements, information gathering/collection and recognition of indicators and warnings, processing and collation of information, intelligence analysis and production, intelligence/information dissemination, and evaluation.

- Management and Administrative Capabilities
  This section outlines a set of operating tenets and governing principles for the fusion center. Technology policy should be driven by the outcome of this analysis. It addresses issues of security, privacy, training, staffing, facilities, and infrastructure. Additionally, it addresses the issues of funding and budgets.
- Noncategorized/Optional Capabilities
  This section outlines considerations for other fusion center capabilities that can be enabled by technology. Decisions as to the priority and criticality of these areas will be determined by the defined mission and function of the fusion center.

Additional relevant sections of the *Defining Fusion Center Technology Business Processes: A Tool for Planning* include:

✪ **Creating the Business Architecture Framework** (Chapter 4)

The business architecture is an integral component of the fusion center's enterprise architecture (EA) framework. It identifies the capabilities, products, services, and value the organization supplies to the "market" (that is, to its external stakeholders or customers), as well as the business processes, roles/responsibilities, agreements, and policies necessary to support the organization's mission, vision, and strategic goals. The business architecture framework provides a structure for defining, describing, and organizing the business processes of the fusion center.

This section provides guidance to the fusion center in the following subsections:

Step 1: Describe the Business Process

- Map Business Processes (by person-intensive and compute-intensive types)
- Identify Associated Capabilities (core capabilities and fusion center additions)

Step 2: Create a Template for Each Associated Capability

Step 3: Flowchart the Process

Finished Framework

✪ **Implementation Considerations/Next Steps** (Chapter 5)

This section provides the fusion center with guidance as to the considerations for planning and support in augmenting its implementation efforts. This section summarizes points that should be considered by the fusion center in the development and execution of its implementation plans.

This section provides guidance to the fusion center in the following subsections:

- Training
- Technology Assistance
- Consultants
- Governance
- Acknowledging That Candidate Technologies Do Support Business Processes

Most substantially, the framework provided in the *Defining Fusion Center Technology Business Processes: A Tool for Planning* will provide a business process view of the critical capabilities of the fusion center. This will, in turn, provide substantial value in the development of a technology strategy that can be utilized to effectively structure information, solution, and technology architectures and, ultimately, provide the ability to perform a business case assessment of future technology initiatives.

3. Technology Strategy and Implementation Planning

As discussed in the previous section, the first step in the development of a responsive technology strategy is to define the business architecture. The mission and critical success factors for the fusion center should also be defined, and the operational priorities should be established. Operational priorities should be based on the capabilities and/or functions of the center that are considered mission-critical, such as detecting and preventing terrorist events; supplying "all-crimes" and "all-hazards" intelligence data to law enforcement and public safety agencies; and supporting emergency management and response operations prior to, during, or after major incidents. Utilizing available fusion center reference materials can enhance the assessment and definition of operational priorities in the fusion center. A complete listing of these resources can be found in the *Fusion Center Technology Resources Road Map: Elements of an Enterprise Architecture for State and Major Urban Area Fusion Centers* document.

The fusion center technology needs should next be developed to meet the needs of the highest operational priorities within these identified functional areas. Although technological solutions can enable capabilities across the center's functional spectrum, investment and expenditure typically require that limited resources be focused on areas of highest potential impact. The only way to ensure a responsive technology strategy is to ensure alignment with the needs of the fusion center.

Figure 1.0 depicts a four-stage methodology for developing a comprehensive technology strategy and implementation plan. Key segments include the development of a future enterprise architecture, the coordinated assessment of the current technology environment, the development of a set of strategic imperatives and a portfolio of strategic technology initiatives, and the integration of the portfolio into an implementation strategy and plan. This methodology can support the development of a technology, strategy, and implementation plan that can be used either by fusion centers that are in a start-up situation or those that are already equipped with technology services.

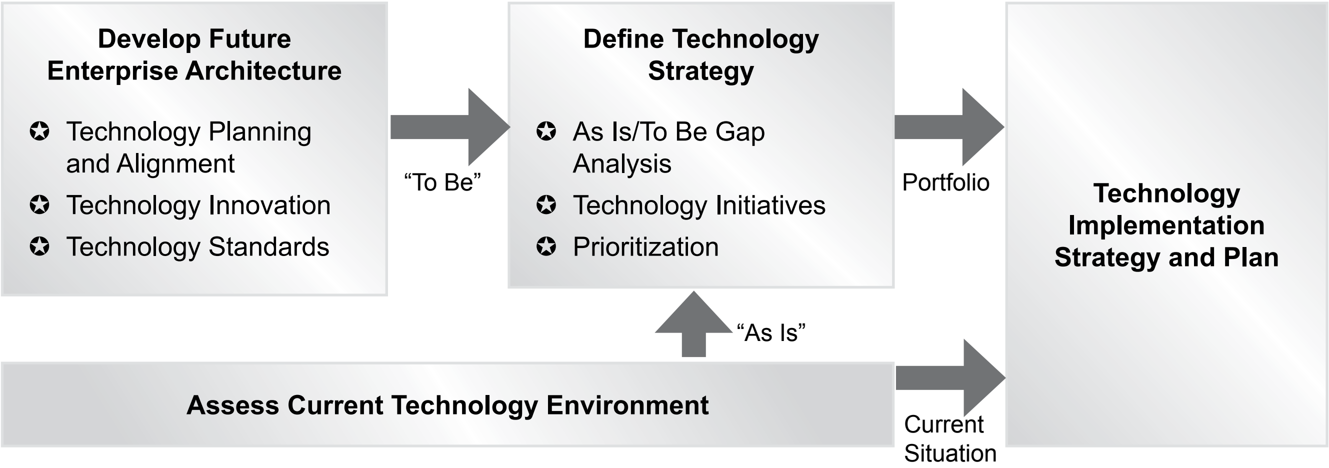
3.1 Develop Future Enterprise Architecture

The *Technology Planning and Alignment* function of enterprise architecture establishes a future vision for the technology portfolio (applications, infrastructure, information exchanges, etc.) that aligns with business strategy and ensures that technology investment decisions move the organization ever closer to achieving this vision.

The *Technology Innovation* function of enterprise architecture provides a mechanism for research and development into new technologies that could increase the organization's efficiency or enable new business capabilities.

Figure 1.0

Technology Strategy and Implementation Planning


Develop Future Enterprise Architecture
✪ Technology Planning and Alignment
✪ Technology Innovation
✪ Technology Standards
"To Be"
Define Technology Strategy
✪ As Is/To Be Gap Analysis
✪ Technology Initiatives
✪ Prioritization
Portfolio
Technology Implementation Strategy and Plan
"As Is"
Assess Current Technology Environment
Current Situation

The *Technology Standards* function of enterprise architecture reduces unnecessary (and potentially wasteful) variation in the technology portfolio by establishing and enforcing best practices. Each of these functions is a necessary component in effective governance of a fusion center's technology portfolio. While not an exhaustive list, the standards initiatives described below provide highly relevant applications for fusion centers.

National Information Exchange Model (NIEM)—NIEM provides a common vocabulary of terms that can provide an information exchange platform allowing different systems to communicate without the development of custom or "stovepipe" solutions for this purpose. NIEM exchanges exist for many of the frequently utilized law enforcement information sharing transactions and can be leveraged by fusion centers to effectively enable information sharing across internal systems, as well as with other partners and outside jurisdictions. NIEM also forms part of the Information Sharing Environment (ISE) Baseline Data View for the ISE Architecture and is the basis for developing ISE functional standards under the Common Terrorism Information Sharing Standards (CTISS) program. Additional information on NIEM is available at www.niem.gov.

Federated Identity and Privilege Management—Federated identity solutions such as the Global Justice Information Sharing Initiative (Global) Federated Identity and Privilege Management (GFIPM) program provide a framework for identification/authentication, privilege management, and audit to access fusion center applications. GFIPM can be utilized to ensure that security and authentication policies are enforced throughout the organization since it provides the definition and management of access privileges to the applications and data contained in the fusion center applications and databases. It also provides the efficiencies of a single sign-on protocol for all authorized fusion center system users, avoiding redundancy and providing cost-reduction savings. Additionally, eXtensible Access Control Markup Language (XACML) provides a standards-based infrastructure for exchanging information about the access control and privacy policies of protected resources in terms of the elements in the metadata model. Fusion centers can leverage Security Assertion Markup Language (SAML), which is an XML-based framework for specifying authentication information about a user. It allows for assertions to be made regarding the identity, attributes, and entitlements of a user. These assertions are passed from one business entity, partner company, or application to another. The audit aspect of GFIPM helps determine what information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data access and management practices.

Justice Reference Architecture (JRA)—The Global JRA is a reference architecture that provides a proven template solution and a common vocabulary with which to discuss implementations, often with the aim to stress commonality. It leverages the best practices of industry and specifically the OASIS Reference Model for Service-Oriented Architecture (SOA). The JRA, based on long-time industry standards and best practices, links the various standards available, such as NIEM and GFIPM, and provides a consistent, uniform approach to managing technology resources to support information sharing. It also supports the necessary linkage between fusion centers and the overall ISE Architecture supporting nationwide terrorism information sharing. Deliverables from the JRA project can assist with developing business architecture (e.g., service identification and design guidelines), information architecture (service modeling guidelines), and technology and solutions architecture (execution context guidelines, service interaction profiles) components. The JRA approach utilizes a cohesive or natural grouping of technologies, standards, or techniques in meeting those service development requirements.

The execution of the first stage of the methodology will result in a multidimensional view of the future, or "To Be," enterprise architecture. While this methodology focuses primarily on the Technology and Solutions architecture components, it is important to mention all for context.

Business Architecture (external): Identifies the capabilities, products, services, and value the organization supplies to the "market" (that is, to its external stakeholders or customers); often, this information is represented in a strategic plan that articulates the organization's mission, vision, and strategic goals.

Business Architecture (internal): Identifies business processes, roles/responsibilities, agreements, and policies necessary to support the organization's mission, vision, and strategic goals.

Information Architecture: Establishes the meaning, location, and ownership of data stored and managed within the organization in support of its mission, vision, and strategic goals and identifies the semantics and structure of information exchanges that the organization performs with external partners.

Technology Architecture: Identifies the technology infrastructure necessary to support the organization's mission, vision, and strategic goals; infrastructure generally includes networks, devices (server computers, workstation computers, mobile devices, etc.), storage, physical plant (floor space, climate control, power, etc.), provision for business continuity (backup power, disaster recovery, fire suppression, etc.), and provision for physical security (access control, intrusion detection, etc.).

Solutions Architecture: Applications and automated work flows that support the organization's mission, vision, and strategic goals.

3.2 Assess the Current Technology Environment

This stage is required as an integral and parallel activity with the development of the future enterprise architecture stage. It applies to fusion centers already utilizing technology and looking to develop and/or update their technology strategies and should encompass all installed and planned technology components. The results of this step will form the "As Is" view of the enterprise and will be used to conduct the "gap analysis" step.

This stage also provides a view into defining future system requirements based upon current utilization of technology. They will provide a baseline for determining the needs for the "To Be" components of the enterprise architecture:

Business Architecture: Understanding of the current business architecture will play a key role in helping all current business processes to be taken into account in the development of the business architecture, as well as to identify the current application solutions supporting these processes and functions.

Information Architecture: Fusion centers manage information in a variety of forms. Information sharing partnerships also exist today. Each of these information management activities will provide requirements and insights into the development of an integrated information architecture design and capability.

Technology Architecture: The current technology architecture provides a view into all of the components supporting the application solutions in operation. Current technology components should be utilized to help define requirements for the future technology architecture requirements.

Solutions Architecture: Current operational and planned application solutions provide and/or will provide direct support to existing fusion center business functions. As such, these current and planned application solutions should be utilized to help define requirements for the future solution architecture components.

In addition to the significance of the current environment analysis in defining future requirements, this stage will provide the "As Is" view of the fusion center architecture for developing the technology strategy and portfolio of initiatives described in the next section.

3.3 Develop the Technology Strategy

The technology strategy will help to define the needs and priorities for application solutions and technology for the fusion center. It will begin with the *Gap Analysis* between the current “As Is” situation of the fusion center’s technology environment and the future “To Be” architecture. The purpose of the gap analysis is to define the needs for technology capabilities and services required to advance the fusion center’s mission.

The identified needs should then be organized into a set of defined *Technology Initiatives.* These initiatives will include a definition of the purpose, function, business process supported, and capabilities enabled. A summary cost of implementation should also be developed for comparison purposes. The technology initiatives should seek to leverage solutions available via national standards and technology initiatives, specifically those supported by Global. Particular attention should be paid to policy considerations that affect technology, such as adequate security controls and protections of privacy and civil liberties for individuals that may be affected by the system, as well as information sharing and communications policy alignment with the fusion centers’ broader policies.

The final step in this stage is the *Prioritization* of the technology initiatives. Each fusion center will have its own definition of “mission” and set of business priorities. In this step, it should be recognized that all of the technology initiatives identified are not likely to command the same priority and resources. As such, a formula for assessing the business value of each should be developed. This formula should consider the value of the initiative to fusion centers in executing their mission (i.e., support to mission-critical operational priorities, impact on operational improvement, impact on budgets, and affordability). This formula should be comprehensive and include not only the short-term costs for acquisition and implementation of application and technology solutions, but it should also consider the sustainment costs for operations and maintenance and the cost for retaining qualified technology management resources.

The results of this step will be a strategically significant portfolio of technology initiatives for funding consideration. This portfolio will provide the direction and guidance for the fusion center’s technology implementation strategy and plan.

3.4 Technology Implementation Strategy and Plan

As the technology strategy and portfolio of initiatives are solidified, an implementation strategy and plan can begin to be formulated. Implementation of each initiative should follow a phased approach and should be managed as an independent project. Each project, while a part of a larger fusion center technology portfolio of initiatives, should be managed according to project plan. A summary of typical project phases includes:

Project Planning—Encompasses project goals, activities, resources, and timelines. Prepared at the outset of the project, the plan is utilized to manage project execution.

System Design—Defines and documents the requirements and design aspects of the application solutions and technology architectures to support fusion center operations. Project-level system designs should support a larger “enterprise” design and architecture for the fusion center.

System Development/Acquisition—Manages the activities to build or buy a solution based upon the requirements specified via the system design phase. Most often, this will include a decision to acquire a commercially available product. However, certain application requirements may be best addressed via development. As time goes on, the volume of commercially available products will increase.

Implementation—Focuses on the technology deployment and system start-up activities. Typically included in this phase are system deployment, system testing, user acceptance testing, user and technical training, and “go-live” operation.

Maintenance—Typically indicates completion of the project and includes postimplementation reviews and the ongoing support and maintenance of the application and technology solutions. Once these reviews are complete, the fusion center data center operations should be prepared to take over support of the application and technology components.

These phases are typically executed in an iterative mode as a method to test the viability of design and development theories via implementation experiences.

4. Fusion Center Technology Framework

The fusion center technology framework should consider the *Information Sharing Environment Enterprise Architecture Framework* (ISE EAF). The ISE EAF assists fusion centers in establishing the relationship between mission/goals, business and information, and technology and transitional strategies through analysis of current environment and future environment.

The architect's perspective of the ISE EAF is broken into four partitions, as shown in Figure 2.0. The implementer's perspective, which should be utilized by the fusion center, is divided into four components, as shown in Figure 3.0.

From the architect's perspective, the ISE EAF is broken into the following four partitions:

Business Partition: Identifies the performance drivers and desired outcomes, business functions, processes, and information flows that facilitate information sharing in the ISE.

Data Partition: Identifies and describes the data required to enable the ISE business processes through the functional standards of the CTISS; defines universal core vocabulary and information exchange structures for sharing information across the various ISE business processes.

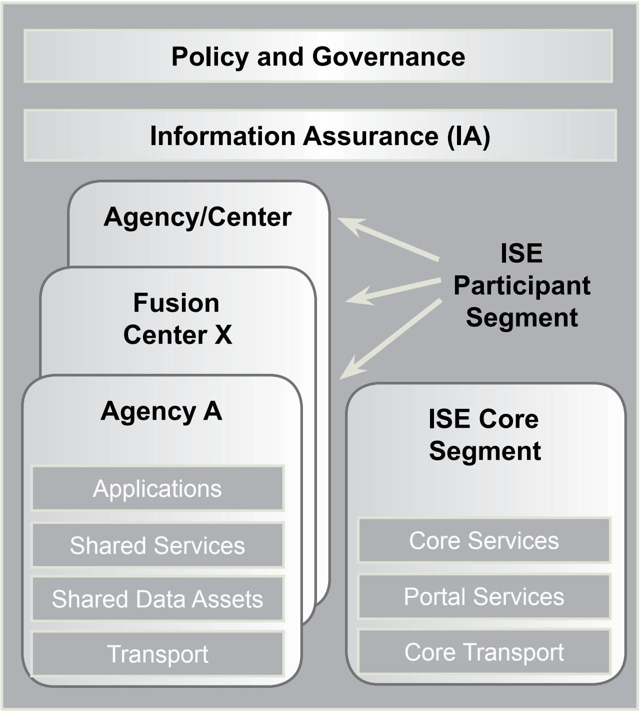
Application and Service Partition: Identifies and describes the software applications and service components that support the business processes; includes Core Services and Portal Services used by all ISE participants, shared services provided by a participant for use by others, and the actual data assets (e.g., databases) to be shared.

Technical Partition: Identifies the technologies, technical standards of the CTISS, and patterns used to implement the applications and services.

Figure 2.0

Business Partition
Data Partition
Application and Service Partition
Technical Partition

Figure 3.0



As shown in Figure 3.0, the ISE recommends that fusion center frameworks be based on four components:

- ✪ Applications
- ✪ Shared Services
- ✪ Shared Data Assets
- ✪ Transport

The above diagram portrays the high-level information sharing framework. This framework is intended to satisfy the goals and requirements of information sharing by identifying specific standards, guidelines, and infrastructure requirements for any group of fusion center partners interested in sharing information among themselves. The solutions described in the tiers below will operate within this framework of the implementer's perspective.

4.1 Applications (Mission Support)

While many of these applications are routinely found in most business environments, they are important for fusion center operations.

Office Automation—Electronic Mail

E-mail is the common linkage between organizations and is used to communicate and track items of interest.

Office Automation—Word Processing

Word processing supports the production of text documents, including bulletins, fact sheets, investigative summaries, and analytical reports.

Office Automation—Spreadsheets

Spreadsheets are utilized to organize numerical data in a column-and-row format for summarization and comparisons of data and data charting.

Office Automation—Presentation Software

This software is required to produce professional-looking slide show presentations, with the capability to incorporate text, photographs, graphics, video, and animation.

Office Automation—Data Visualization

Data visualization supports the automatic display of information in formats (e.g., graphs, pie charts) and is sometimes part of a larger software application, such as spreadsheet software.

Office Automation—Graphics Software

Graphics software extends graphics capabilities beyond word processing and spreadsheet software, thereby providing a complete and detailed representation of the applicable data, concepts, or conclusions using graphic arts.

Office Automation—PDF File Creation Software

PDF files can be viewed and printed on operating systems such as Mac OS X, Microsoft Windows, and UNIX, thereby facilitating the sharing of information. PDF files can also be locked down to prevent tampering with the final product.

Office Automation—Publishing Software

This software is utilized to produce professional-looking publications, such as newsletters or bulletins.

Antivirus Software

This software is utilized to identify, neutralize, or eliminate malicious software.

Finance and Administrative Management Systems

As operating organizations, fusion centers require the ability to prepare and manage operating budgets, manage center personnel, and track assets. Fusion centers have a multitude of financial and administrative management systems from which to choose.

4.2 Applications (Mission-Critical)

Suspicious Activity Reporting

Fusion centers should have an application that will receive suspicious activity reporting from multiple sources—including public safety agencies, commercial organizations, and the public—and store such reports in a database where subsequent analysis can be conducted to validate them or determine that the reports are unfounded. This application should also provide for the dissemination of vetted suspicious activity reports to appropriate federal agencies, state/local agencies empowered to act on the reports, and the originators of the reports to provide feedback on their disposition. This application should support the transmission of information exchanges as defined in the ISE-SAR Functional Standard and associated IEPD issued by the Program Manager for the Information Sharing Environment.

Case Management

It is recommended that a case management/records management system be implemented to track investigations, leads, and activities conducted in support of investigations to preserve records for investigative and prosecutorial purposes, as well as to manage work flow of investigators and analysts.

This application must be able to integrate closely with the suspicious activity reporting application, avoiding any duplicate data entry or requirement for separate data management or maintenance. However, the case management system must be flexible enough and able to record all information related to the processing of cases in sufficient detail to support prosecution. In smaller fusion centers, the suspicious activity reporting and the case management system may be provided by the same software product.

These applications should also support the special handling of intelligence information as outlined in 28 CFR Part 23 and other provisions of law and policy that apply. The case management system should have the capability of handling different levels of access based on the clearance level of the user, as defined and reflected in the security management software and hardware.

Each fusion center's intelligence case management system should support the full range of analytical activities, types of data, and work products defined by the fusion center. An effective case management system will either have the capabilities outlined below or be integrated with specific software products so that duplicate data entry and data management are not required. In particular, the case management system should have the ability to provide these functions or be integrated with separate software that does so.

Communications/Telephone (Toll) Record Software

Structured information collected from telephone billing systems (including cellular phones), pen registers, and dialed number recorders must be organized for analysis. Communications/telephone records software aids in the analysis of communication and telephone information, including source or destination of a call; the times of calls; and the dates, frequency, sequence, patterns, and duration of calls to/from one or many telephones. The functionality provided by this type of software may be included in the intelligence case management application previously discussed.

Statistical Analysis Software

Statistical analysis software enables the user to create descriptive statistics, which in turn allows for the summarization and analysis of qualitative and quantitative data, using calculations such as frequency, percent change, mean, median, mode, and measures of variance (standard deviation and standard error).

Business Intelligence Software (Analytics)

Business intelligence software allows the analyst to find patterns and relationships in extremely large volumes of information, as may be contained in the data warehouse built from multiple sources. This software extends the analyst's ability to find patterns derived from more data than can be managed by an individual but also automates the analysis to find correlations not intuitively obvious. Fusion centers require the ability to apply these techniques to both structured and unstructured data and to include searches across multiple data sources and systems.

Timeline/Flowcharting

A timeline/flowcharting can support tactical or strategic planning, as well as investigations. Timeline software tools can visually show the order of events for an identified or suspected crime. Flowcharting can visually demonstrate the flow of goods within a criminal enterprise. A timeline/flowcharting can also serve administrative purposes, such as visual project tracking.

Link Analysis

Link analysis supports the linking of associated information from one or more structured data sources and displays the links between entities graphically. This type of software can also include a timeline or flowcharting capability. Link analysis software can visually show relationships, including association analysis and hierarchical relationships (e.g., organized crime hierarchies).

Intelligence Products Generation

Applications are needed to generate the baseline set of intelligence products. Each intelligence product should be identified, and each product should have an identified audience and dissemination policy. Products may include monthly strategic reports, daily situation reports, tactical reports, and critical issue reports as necessary. Initially, distribution may be through paper copy, but the software acquired should be capable of supporting the automated distribution of such products using available and secure networks and distribution facilities.

Mapping/Geographic Information System (GIS)

A GIS is utilized to display geographic data using visual points or shapes corresponding to specific locations or areas on a map to aid in crime and critical infrastructure and key resources (CIKR) mapping and strategic intelligence charting. Obtaining a spatial analysis capability includes both mapping (display) software and the underlying map data. The GIS must be capable of handling multiple, different layers of information on street centerline maps.

4.3. Shared Services

The technology components listed in this tier offer a basic list of some of the shared services that support generalized functions, as well as provide the required operating and data sharing foundation for capabilities to be implemented.

ISE Shared Spaces

The ISE Shared Spaces provide authorized users with a mechanism for the collection, storage, and management of data relevant to terrorism information. The ISE Shared Spaces concept is a key implementation approach for developing trust and communitywide information sharing across the entire ISE. The ISE Shared Spaces concept is utilized in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI creates a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related. Using a distributed search capability designed to access SAR data stored in locally owned, similarly configured servers, the shared spaces concept has proven to be a successful solution to the sharing of terrorism-related information between agencies. Access to the NSI's Shared Spaces may be made via Law Enforcement Online (LEO), the Regional Information Sharing Systems® secure intranet (RISSNET™), and the Homeland Security Information Network (HSIN). The FBI's unclassified system, known as eGuardian, will also serve as an ISE-SAR Shared Space, and it is available to state, local, tribal, and federal law enforcement entities via LEO. Additional information on the NSI ISE Shared Spaces is available at http://www.ise.gov/pages/sar-initiative.html.

National Crime Information Center (NCIC)

The NCIC is a computerized database that provides fusion center analysts with a system for making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. Additional information on NCIC is available at http://www.fbi.gov/hq/cjisd/ncic.htm.

National Data Exchange (N-DEx)

N-DEx provides fusion center analysts with the ability to detect relationships between people, places, things, and crime characteristics; to link information across jurisdictions; and to "connect the dots" between apparently unrelated data without causing information overload. This capability will occur primarily in the realm of structured data but can also include unstructured data. Additional information on N-DEx is available at http://www.fbi.gov/hq/cjisd/ndex/ndex_home.htm.

Terrorist Screening Center (TSC)

The TSC supports federal, state, local, territorial, and tribal law enforcement agencies by making Terrorist Identities Information accessible through NCIC to law enforcement officers, adding resources to the fight against terrorism. Additional information on the TSC is available at http://www.fbi.gov/terrorinfo/counterrorism/tsc.htm.

4.4. Shared Data Assets

Relational Database

The relational database provides the ability to organize data in a format of tables (rows and columns) arranged in relation to commonalities and relationships among the data. This tool can also be used for record keeping and for storage of large quantities of data.

Metadata Repositories

Metadata repositories store metadata, which can help retrieve the relevant data later or share with other business partners.

Federated Search—Public Information Database Resources

The purpose of this data asset is to provide fusion center analysts with access to multiple sources of public data via a single comprehensive search facility.

4.5. Transport

Data Communications and Network Connectivity

Access to various networks is essential for fusion center operations. Fusion center personnel should obtain access to the Internet and the state's Law Enforcement Information Network. There are multiple Sensitive But Unclassified (SBU) national network communications resources available to fusion centers, including the Homeland Security Information Network (HSIN), the FBI Law Enforcement Online (LEO), and the Regional Information Sharing Systems (RISS) secure intranet (RISSNET).

System security management hardware and software are required to provide for authentication and authorization of individual users of fusion center systems, consistent with the specifications defined in the Global Federated Identity and Privilege Management documentation. System security should provide a single sign-on capability for all systems and applications consistent with access privileges of each user. The security management should also support the policies and regulations developed for handling controlled unclassified information in accordance with national policy statements.

OSI Network Management Model

This network management model should be utilized to manage the network infrastructure. This model falls into five categories and is also referred to as FCAPS:

Fault Management: This area addresses the detecting, logging, and correcting of the network faults.

Configuration Management: This area addresses the system configuration and change management of the networks.

Accounting: This area addresses the data analysis side of the network (i.e., network utilization, user access, etc.).

Performance Management: This area addresses the efficiency of the current network and addresses the future needs to support business needs.

Security Management: This area addresses the access control to networks. It also focuses on analysis of threats to existing networks and builds policies to stop them.

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