

Guideline 7

Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems. Use the U.S. Department of Justice's (DOJ) Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) and the National Information Exchange Model (NIEM) standards for future database and network development, and consider utilizing the Justice Information Exchange Model (JIEM) for enterprise development.

Interconnectivity

Justification

Law enforcement entities must communicate. The ultimate goal is to eliminate barriers to communications and intelligence development and exchange. Communication barriers come in a number of forms—e.g., incompatible or disparate computer systems, lack of trust, lack of interoperability, lack of a common terminology, and lack of funding. Centers should establish formal protocols (policies and procedures) and standards to enhance communications, as well as create effective and efficient vehicles for exchanging information. Center personnel and leadership should communicate frequently and be responsive to the needs, concerns, and ideas of both internal and external partners. The information contained in this guideline pertains to verbal, written, and electronic communications.

It is recommended that fusion centers leverage existing systems and those currently under development and allow for future connectivity to other state, local, tribal, and federal systems. Furthermore, centers should be aware of and educated on Global JXDM. Any new database development should be Global JXDM-compliant and meet existing standards. It is important to note that



DOJ and the U.S. Department of Homeland Security (DHS) are integrating the use of Global JXDM into grant recipient criteria.

Global JXDM is a comprehensive product that includes a data model, a data dictionary, and an XML schema that is sponsored by DOJ. Its development is supported by the Global XML Structure Task Force (GXSTF), which works closely with researchers at the Georgia Tech Research Institute (GTRI). The Global JXDM is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner. The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, Global JXDM enables access from multiple sources and reuse in multiple applications.

Issues for Consideration

- When establishing connectivity and communications, consider:
- Striving for compatibility not commonality.
- Including both technical and managerial portions of connectivity.
- Using Web-enabled technology when available.
- Using a distributed structure when appropriate.
- Developing mechanisms to communicate internally with participating agencies.
- Developing a policy to ensure proper communication with leaders and policymakers, the public and private sector, media, and citizens.
- Ensuring secure and redundant communications.
- Establishing an electronic notification capability for fusion center participants.
- Maintaining a stand-alone security system (mobile).
- Implementing a communications plan.

- Identifying the requirements for private sector and public safety systems and networks.
- Adhering to need-to-know/right-to-know stipulations.
- Developing outreach material to help increase awareness among policymakers, media, and citizens.
- Conducting training on proper communication and center policy.
- Meeting regularly with personnel and offering intelligence exchange sessions.
- Remembering that communication goes beyond just in-house communication.
- Incorporating the protocols for communication and information exchange in the MOU (Guideline 5).

Justice Information Exchange Model

It is important to document and analyze information exchange at the planning stage of a project and to create a blueprint at the enterprise level (among agencies, levels of government, and a variety of disciplines) for electronically sharing data that capitalizes on efficiency, accuracy, and timeliness. This is regardless of whether interfaces between systems for sharing intelligence consist of simple queries and responses or are more sophisticated transactional processes that build central index entries or populate data warehouses. This design should be created by business experts from the participating organizations, under the direction of policy leaders and with the assistance of technologists. It should be based on a disciplined examination of current business practices, existing technology, and paper and electronic exchange of intelligence that already is occurring.

The Justice Information Exchange Model (JIEM) can assist fusion centers in performing these important tasks. Created by SEARCH, The National Consortium for Justice Information and Statistics, and supported by the Office of Justice Programs' (OJP) Bureau of Justice Assistance (BJA), JIEM documents the processes, triggering events, and conditions that govern information exchanged at the enterprise level. It models the data that flows or should flow between organizations. JIEM was developed to collect requirements from practitioners for justice information sharing initiatives, specifically to assist justice system leaders in analyzing and documenting existing information exchange at the enterprise level. JIEM was also developed to assist in designing new electronic exchange processes as a part of an integrated justice initiative and in adopting and implementing national business, data, and technology models to save time, effort, and money. It is a conceptual framework that presents the flow of information between agencies, defines the key events that trigger the need to share information, identifies the agencies involved in the exchange, and describes the nature of the information exchange, irrespective of whether one is analyzing a justice or nonjustice system exchange. JIEM helps justice and public safety practitioners to articulate requirements that can be communicated to technologists who develop systems and interfaces.⁴⁵

JIEM is linked with DOJ's Global JXDM, allowing easy importing of model components to design electronic documents. Soon it will be linked with the ability to import and export XML schema

⁴⁵ Additional information on JIEM can be found at www.search.org/programs/info/jiem.asp.

and other Information Exchange Package Documentation (IEPD) artifacts that are essential to implementing the Global JXDM. This will eventually enable justice agencies to seamlessly generate (and, if need be, regenerate) Global JXDM-compliant information exchanges from the business rules encapsulated in JIEM, ensuring that they can be rapidly adapted to the needs of an increasingly dynamic environment. JIEM is also being enhanced to support the exchange of information, not only within domains (as in the justice domain today) but between different domains—such as justice, emergency management, transportation, and intelligence—in support of emerging organizations, such as fusion centers.⁴⁶

National Information Exchange Model

The U.S. Department of Justice's (DOJ) Office Justice Programs' (OJP) Bureau of Justice Assistance (BJA) is collaborating with DHS to utilize the Global JXDM as the base for the deployment of the National Information Exchange Model (NIEM). NIEM will provide the foundation and building blocks for national-level interoperable information sharing and data exchange that will integrate the public safety and private sector entities to the already established law enforcement information exchange. The tentative date for NIEM to be operational is October 2006.⁴⁷

In addition to NIEM and JIEM, other options for interconnectivity include developing and utilizing a secure Internet site to post alerts, calendars that may include training information and significant dates, and a chat interface. Another option is a Web portal to connect the fusion center with private sector and public safety partners that will allow for a single sign-on and can provide situational awareness reports, threats, and warnings. It also has the capability for e-mail notifications. Interconnectivity also includes face-to-face communication, including regular meetings with other intelligence centers to share information and intelligence. Interconnectivity aids in institutionalizing the relationships between the fusion center and the public safety and private sector partners. However, fusion centers and their partners should be aware of privacy issues when developing information sharing networks, systems, or Web sites.

Distributed Versus Centralized Systems

Currently, both distributed and centralized systems are being used successfully for law enforcement information and intelligence sharing. There are benefits and challenges to both models.

A distributed model allows participating entities to control their data. Data is not commingled or housed in a data warehouse. Agencies are responsible for the quality of the data and the accessibility of their information. The distributed structure can streamline policy development and minimize privacy concerns, while providing the same functionality as a centralized model.

⁴⁶ The SEARCH report, *Information Exchange Analysis and Design*, can be found in Appendix E of this report.

⁴⁷ For more information on NIEM, visit www.niem.gov.

The distributed model is also reliable and can maximize resources. Distributed systems are scalable and offer aggregate computer power. However, security issues, resource distribution, demand, and computing power can limit the distributed model.⁴⁸

A centralized system places all information in one location. Collection of information and refreshing of data can be complicated with a centralized structure. However, often the functionality of the centralized system is greater and allows for increased speed.

A white paper prepared by the IJIS Institute provides a comparative analysis of the distributed and centralized system based on five components: cost, governance and data ownership, performance and functions, scalability, and security and privacy. This document is included on the resource CD. Centers should evaluate both structures to determine the best fit. As described above, it is the recommendation of the *Fusion Center Guidelines* that systems be distributed or centralized; however, federal data that contains personally identifiable information should be separate from other types of information the fusion center receives, including public safety and private sector information.

Service-Oriented Architecture

Information sharing is a long-standing practice among justice agencies, particularly within the law enforcement community. As society becomes more mobile, the importance of sharing data to improve police effectiveness grows exponentially. The Web and the technologies that support it have enabled information sharing to go beyond exchanges among specific partners to embrace the whole of the justice community. This includes law enforcement, prosecutors, defense counsel, courts, probation and corrections, and a host of corollary disciplines, such as homeland security, fire, emergency services, health, education, transportation, and motor vehicle licensing. Service-oriented architecture (SOA) incorporates six fundamental principles for the sharing of information in the criminal justice community:

- The architecture must recognize innumerable independent agencies and funding bodies from the private sector through local, state, tribal, and federal governments.
- Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.
- The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.
- Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.
- Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.
- The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

⁴⁸ Texas A&M University Computer Science Department. Introduction to Distributed Systems, 2001.

This concept of design allows the original data owners to control their own data, both in terms of who is allowed to access it and in ensuring the integrity of the data. It allows agencies to retain the investment they have made in their existing systems and at the same time gain access to valuable information contained in other agency systems. It uses the technology of the Internet, which is user-friendly and readily understood by most.

In 2004, DOJ's Global Infrastructure/Standards Working Group (GISWG) published a document entitled *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*. Based on the report, Global recognizes that SOA is the recommended framework for development of a justice information sharing system. The report indicates that a system should be designed and developed around the basic components of the operational procedures or business practices of an agency. These components are then combined into a larger, loosely related structure that, in turn, can be combined into an even larger entity. The SOA design must be available to all agencies and support the evolution of change and new technology, with support for start-up, maintenance, and future upgrades to the information sharing systems that are based on the SOA framework. A complete copy of the report is contained on the accompanying resource CD.

Organization for the Advancement of Structured Information Sharing Systems (OASIS)—Ratified Common Alerting Protocol (CAP)

It is recommended that, where possible, fusion centers use the OASIS-ratified CAP to enable the exchange of emergency alert and public warning information over data networks and computer-controlled warning systems. Using CAP also adds an element of redundancy to the systems and networks. By limiting transport-specific nomenclature, CAP remains fully compatible with existing public warning systems, including those designed for multilingual and special-needs populations, as well as with XML applications, such as Web services. CAP data elements have been incorporated in DOJ's Global JXDM. Other agencies, such as DHS's Federal Emergency Management Agency (FEMA), have embraced the CAP and are in the process of integrating it into all alert and warning systems.

Available Resources on Fusion Center CD

- *A Critical Look at Centralized and Distributed Strategies for Large-Scale Justice Information Sharing Applications* (a white paper prepared by the IJIS Institute)
- *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*, http://it.ojp.gov/documents/200409_Global_Infrastructure_Report.pdf
- Global Justice XML Data Model (Global JXDM), www.it.ojp.gov/gjxdm
- Justice Information Exchange Model, www.search.org/programs/info/jiem.asp
- Model Intelligence Database Policy