



IJIS Institute

Realize the Power of Information



2009

August

Guide to

Information Sharing and Data Interoperability



for Local Communication Centers

Public Safety Data Interoperability Program (PSDI)

Scott Parker

Project Manager, IJIS Institute

Steve Wisely

*Director, Comm Center and 9-1-1 Services
Department, APCO*

Cover photo: City of Richmond, VA

**U.S. Department of Justice
Office of Justice Programs**
810 Seventh Street, NW
Washington, DC 20531

The Honorable Eric H. Holder Jr.
Attorney General

The Honorable Laurie O. Robinson
Acting Assistant Attorney General

The Honorable James H. Burch II
Acting Director, Bureau of Justice Assistance

**Office of Justice Programs
World Wide Web Home Page**
www.ojp.usdoj.gov

**Bureau of Justice Assistance
World Wide Web Home Page**
www.ojp.usdoj.gov/BJA

**For grant and funding information contact
U.S. Department of Justice, Office of Justice Programs Funding Opportunities**
<http://www.ojp.usdoj.gov/funding>

This project was supported by Grant No. 2007-DD-BX-K155 awarded by the Bureau of Justice Assistance. 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 United States Department of Justice.

TABLE OF CONTENTS

1	PURPOSE.....	1
1.1	Abstract.....	1
1.2	Target Audience	1
1.3	Expected Benefits	1
2	THE NEED FOR DATA INTEROPERABILITY IN THE COMMUNICATIONS CENTER... 	2
2.1	What is Data Interoperability?	2
2.2	Need to Share Information Up and Down.....	3
2.3	NIEM and the Value of Information Sharing	3
3	COMMON SCENARIOS	7
3.1	Scenario 1: Existing/Current.....	7
3.2	Scenario 2: Evolving	7
3.3	Scenario 3: Futuristic	7
3.4	Single Agency Environment.....	8
3.5	Multiple Agency Environment.....	9
4	COMMON INFORMATION FLOWS: ORIGINATORS AND RECIPIENTS	10
5	HOW IS DATA INTEROPERABILITY ACHIEVED?	11
5.1	Data Interoperability System Development – The Big Picture	11
5.2	Data Interoperability System Development – Implementation Methodology.....	13
5.2.1	Governance	13
5.2.2	Disparate Systems	13
5.2.3	Custom Interfaces	13
5.2.4	Multiple Standards	14
5.2.5	Lack of Funding	14
5.2.6	Culture.....	14
6	THE PSDI PROGRAM APPROACH	15

7	IMPORTANT TECHNICAL CONCEPTS	16
7.1	Information Exchange Package Documentation (IEPD)	16
7.2	The ANSI Process	16
8	GETTING STARTED: A REAL-WORLD APPROACH TO DATA INTEROPERABILITY	17
8.1	Scope Your Efforts	17
8.1.1	Determine Relevant Data Exchanges	17
8.1.2	Map Relevant Data Exchanges on a Value Graph	18
9	MAKE IT HAPPEN!	21
9.1	Project Governance	21
9.1.1	Establishing a Governance Structure	21
9.1.2	Maintaining a Governance Structure	22
9.1.3	Additional Recommendations.....	22
9.2	Fund the Project	23
9.2.1	Federal Funding.....	23
9.2.2	Grants.....	23
9.2.3	State Administering Agencies	24
9.2.4	Alternative Funding Approaches.....	24
9.3	Your Project Team and Implementation	27
9.4	Selecting Solution Providers.....	28
9.5	Keep it Happening!	29
9.5.1	Improve Processes	30
9.5.2	Cast a Wider Net	30
9.5.3	Evaluate IEPD Enhancements.....	30
9.5.4	Share Experiences with Your Peers.....	30
10	APPENDIX A: IEPD CLEARINGHOUSE.....	31
11	APPENDIX B: APCO INTERNATIONAL AMERICAN NATIONAL STANDARDS (ANS) PROCESS	32
12	APPENDIX C: NFPA STANDARDS	34
13	APPENDIX D: PSDI COMMITTEE MEMBERS / CONTACT INFORMATION.....	35

13.1	PSDI Committee:	35
13.2	Other Contributors	37
13.3	Contact information	37
14	APPENDIX E: THE APCO/IJIS INSTITUTE PARTNERSHIP	38
15	APPENDIX F: ADDITIONAL RESOURCES	39
15.1	JTTAC Training & Technical Assistance Opportunities	39
15.2	IJIS Institute	39
15.3	Institute for Intergovernmental Research (IIR)	39
15.4	SEARCH—The National Consortium for Justice Information and Statistics	40
15.5	Law Enforcement Information Technology Standards Council (LEITSC)	40
15.6	Global Justice Information Sharing Initiative (Global)	40
15.7	Lessons Learned Information Sharing (LLIS)	40
15.8	National Information Exchange Model (NIEM)	40
16	APPENDIX H: GLOSSARY	42
17	APPENDIX I: BIBLIOGRAPHY	45

1 Purpose

1.1 Abstract

This document, authored by the Public Safety Data Interoperability (PSDI) committee, provides managers of public safety communications centers (to include Public Safety Answering Points or any agencies that answer emergency calls) with an overview of the issues and opportunities surrounding data interoperability. It provides practical insights and action-oriented advice for managers looking to enhance data interoperability in their facilities. The PSDI Committee consists of a combination of practitioners and industry representatives and is supported by the Bureau of Justice Assistance, U.S. Department of Justice. The PSDI Project is co-managed by the IJIS Institute and the Association of Public Safety Communications Officials International (APCO).

1.2 Target Audience

This document is targeted to people in leadership positions in public safety communications centers. Both sworn and non-sworn leaders will benefit from the information presented in this document. Managers and directors who are looking to enhance data interoperability between the communications center and its business partners will find a wealth of practical, action-oriented information in this guide.

1.3 Expected Benefits

Over the past ten years, multiple organizations have identified the benefits of exchanging vital information at critical points during the public safety response and/or follow up to an incident. These benefits include streamlining processes, reducing manual efforts, and reducing errors. These benefits translate into being able to deliver services more effectively, saving both time and money and, more importantly, saving lives. We have passed the point of asking, “Is data interoperability necessary?” We should now be asking, “How do we achieve interoperability as quickly and efficiently as possible?”

2 The Need for Data Interoperability in the Communications Center

In the traditional emergency communications center of the past, calls for service typically came in over ordinary phone lines and messages went out to units over a radio frequency. In recent years, with the explosion of the cell phone industry and new technologies such as Voice-Over-Internet Protocol (VoIP), the sources of information are rapidly expanding and changing. Some police cruisers are equipped with cameras that scan license plates of passing vehicles and signal the officer when a hit is made on a stolen car. Major cities are installing similar equipment on bridges and tunnels, along with sensors that are capable of detecting the presence of radiological agents like cesium or cobalt. The data is presently going to command centers, but could, in the future, be channeled to emergency communications centers.

Text messages and cell phone pictures are subjects that often come up in discussions about the next generation of 9-1-1 (NG9-1-1). The challenge, therefore, is to be able to accept these types of data at the communications center.

It has been suggested that there is more computing power in a modern automobile than there is in the average office desktop computer. Vehicles, from small cars to the largest trucks, have sensors that, among many other things, detect speed, performance, and crash velocity. Many of these vehicles have the capability to transmit pertinent information, including voice and GPS coordinates, back to a centralized call center or, in some cases, directly to the nearest emergency communications center through their internal telematics systems.

All of this data, and more, needs to be processed by the Computer Aided Dispatch (CAD) system. But how can such divergent data, coming from so many disparate systems and sources, be fed into an existing CAD system? How do we achieve data interoperability given the need to process disparate data coming into the CAD system, as well as the need to push data out to other public safety systems?

2.1 What is Data Interoperability?

First responders have long struggled with the issues surrounding interoperable communications; until recently, voice interoperability has been the issue of most concern. Today, however, the first responder community has begun to realize the importance of data interoperability. Over the next few years, data interoperability has the potential to revolutionize the role of the public safety communications center. Public safety data interoperability is the capability of the first responder community (law enforcement, fire services, EMS, and the related communications centers) to exchange digital information, in many different formats, using well-defined, highly repeatable business processes. Styles of data interoperability include:

- *Structured* data exchange between the communications center and other related organizations, including police, fire, emergency medical services, emergency operations centers, hospitals, etc. These structured exchanges across agency boundaries are enabled by standards such as the National Information Exchange Model (NIEM), which is discussed later in this document.
- *Unstructured* data exchange between the communications center and the general public, private sector, political leadership, etc. These exchanges are enabled by commonly accepted digital data formats for images, video, audio, text messaging, etc.

Data interoperability requires general agreement, throughout the First Responder community, on a small number of key issues:

- For *unstructured* data exchange, the community should settle on commonly used file formats for images, audio, video, etc.
- For *structured* data exchange, the community must agree on a common vocabulary and grammar (Data Dictionary) to be used to create pre-defined exchange types. When multiple standards exist, a community must agree on one of them.
- For any type of data exchange, the community must develop well-defined business processes that enable data exchanges to be triggered, processed, and monitored from start to finish.

For more information regarding these issues, see “How is Data Interoperability Achieved?” later in this document.

2.2 Need to Share Information Up and Down

Since September 11, 2001, the mission of first responders has expanded to include homeland security considerations. When responding to an incident, public safety personnel can no longer focus solely on traffic mitigation, criminal activity, firefighting, or resolving a medical situation. First responders must now consider the potential for incidents to be terrorism related. Additionally, first responders must be cognizant that, while the situation itself may not be terrorism related, the persons, conveyances, or structures involved may somehow be part of a larger picture involving terrorism, potential terrorist activity, or other crime.

In today’s public safety environment, it is crucial that information be shared, both vertically and horizontally. This information sharing must not be limited to a one-way collection and submission by first responders; critical success is found only in providing relevant information back to first responders.

Information provided to first responders must be timely and accurate to enable first responders to know who and what they may have on the scene. Failing to provide this information accurately and in an appropriate timeframe may result in persons or items of interest being lost or harmed. Additionally, information collected from the scene that may indicate some nexus to homeland security concerns must be shared in real-time in order to enable an appropriate analysis and response. Lastly, it is essential that information sharing in a real-time environment be done with the appropriate attention being paid to privacy and security requirements.

The communications center is a key participant in the intelligence information “gathering and sharing” mission. The communications center should have connectivity and sharing capability both with first responders and with intelligence collection, analysis, and dissemination recourses, whether they are local law enforcement intelligence units or more structured fusion centers. Leveraging emerging standards in intelligence information sharing will enable communications centers’ data systems to assist in the collection and sharing of information with the intelligence centers, and will allow the communications centers to receive critical intelligence information for dissemination to the field.

2.3 NIEM and the Value of Information Sharing

Information is the lifeblood of effective public safety and homeland security. In making a multitude of decisions every day, officials must have immediate access to timely, accurate, and complete

information. Regardless of whether the situation involves a police officer conducting a routine traffic stop, a security officer conducting passenger screening at an airport, or a customs official screening cargo arriving at an international port, effective decision making requires information that often must be shared across a broad landscape of systems, agencies, and jurisdictions. The challenge is clear – how do we build bridges that span the wide array of computer systems operating in various agencies to share information for improving public safety and homeland security?



The National Information Exchange Model (NIEM) is designed to enable government and industry to address this problem. NIEM defines data exchange standards for information that is commonly shared across the broad justice, public safety, emergency and disaster management, intelligence, and homeland security enterprises. The standards derive from actual exchanges that support the day-to-day operations of officials at all levels of government, as well as the private sector and the general public. In addition to developing exchange standards, NIEM also provides structured methodologies, technical tools for building exchanges, training, technical assistance, help-desk support for users and developers, and an effective governance structure that encourages the active involvement and input of users and practitioners from all levels of government and industry.

Ensuring public safety and homeland security is the most fundamental objective of most information sharing initiatives. The value of sharing accurate, timely, and complete information across the entire enterprise cannot be overstated: getting the right information to the right people all of the time means that officials will be properly equipped to make informed decisions in planning for, preventing, or responding to terrorist attacks, natural disasters, large-scale and organized criminal incidents, and maintaining effective day-to-day operations. Timely access to quality information enables better decision making, which can easily translate into saving lives and protecting valuable infrastructure. Standards-based information sharing can also mean quicker access to, and better understanding of, the data that crosses system, agency, and jurisdictional borders.

First responders, analysts, agency representatives—those who must share information in mission-critical jobs on a daily basis—are the people who are building the NIEM standards; this means they will not have to reenter the same data multiple times, delay critical decisions for lack of data, or take action based on inaccurate or incomplete information. Further, NIEM information sharing standards will accelerate systems development, mitigate risk by enabling developers to build to common standards and reuse common components, and promote agility in responding to the evolving requirements to share data in new and innovative ways.

The ability of government personnel to effectively serve customers and the general public, and to deliver positive outcomes, hinges on the availability of appropriate and accurate information. Access to such information ensures that decisions are made and assistance provided as quickly as possible. Consider the following examples that describe how NIEM could help to improve the quality of government services:

Preventing Terrorist Attack – As documented by the *9/11 Commission Report*, our inability to share real-time intelligence and criminal justice data contributed to the terrorists’ success. Even today, fusion center personnel must often overcome this deficit by sharing information via phone calls and personal contact. NIEM will provide value by enabling criminal justice and intelligence systems to share data in real time. With the knowledge harvested from broad information sharing, fusion center personnel and others within the intelligence and law enforcement community will be better equipped to identify potential threats and prevent future terrorist attacks. Recognizing this, many fusion centers including those in Michigan, New York, and Virginia have endorsed NIEM as their standard for data exchange.

Responding to Disaster – In disaster situations, first responders and emergency personnel must be able to effectively communicate and remotely share information. During last year’s battle with wildfires in the western United States, residents of a threatened community received conflicting directives from law enforcement and fire department personnel. NIEM data exchange standards can help to link law enforcement agencies, fire departments, and other critical information sources required by first responders, such as medical, environmental, and transportation personnel. In this way, NIEM serves as a vital tool to help improve the speed and effectiveness of our nation’s disaster response.

Fighting Crime and Administering Justice – Decision making throughout the justice enterprise depends on immediate access to timely, accurate, and complete information. When a law enforcement officer in the field stops a suspect, a judicial officer makes a bail or sentencing decision, or a correctional official determines whether to hold or release an individual, their decisions rely, in large part, on information collected and shared between multiple agencies and jurisdictions. Incomplete information regarding a subject’s identities, legal status, criminal record, and warrant status, along with information on whether or not the individual is a danger to the public or himself/herself, puts the officers and the public at risk and can result in tragedy. NIEM provides the data-exchange standards and support mechanisms to facilitate broad information sharing for effective decision making.

Cutting the Cost to Share Information – NIEM embraces collaboration with preexisting standards and can help organizations avert many of the risks inherent in developing and adopting new standards. Since NIEM’s components and exchanges are reusable, the time and cost necessary to deploy new information exchanges are significantly reduced. Pennsylvania has implemented a standardized, repeatable process for all integrated technology solutions, reducing the message exchange development process from nine months to six weeks. This action may have resulted in millions of dollars in taxpayer savings. The Missouri State Court Administrator reports that development time for exchanges has been cut by 50 percent since the adoption of NIEM-related standards.

Increasing the Accuracy and Speed of Information Sharing – Government information is stored in thousands of disparate applications and databases. The process of accessing, aggregating, and analyzing relevant data to respond to an emergency, make an immigration decision, issue a state identification card, or solve a crime is time-consuming, costly, and too often fraught with errors. Consider the officer assigned to the case of two slain New York City detectives, who contacted Pennsylvania authorities to request information on two suspects. Using NIEM-related exchanges, officials were able in just a few hours, rather than over days or weeks, to gather and forward information on the suspects, including birthdates, social security numbers, fingerprints, photos, and vehicle information.

Reducing Administrative Burden – Agencies at all levels of government are challenged with responding to increasing demands for their services. Yet many of these government entities spend valuable time manually rekeying data into their systems. For example, Orange County, Florida, has reported that eliminating the redundant entry of arrest information saves an estimated \$5 million to \$7 million per

year. NIEM provides a means to eliminate data entry redundancy—freeing resources to perform more valuable services for the public.

Significant progress is being made in building and implementing enterprise-wide information sharing standards through the NIEM program. NIEM version 1.0 was released in October 2006; June 2007 saw the release of an expanded version 2.0, which harmonizes key components across an expanded range of domains— Emergency Management, Immigration, Infrastructure Protection, Intelligence, International Trade, Justice, and Person Screening. Pilot programs are well under way for building and implementing NIEM-conformant exchanges in a variety of operational and mission-critical venues. NIEM is gaining significant traction by expanding adoption and development among agencies at all levels of government and with private industry and solution providers.

NIEM is a business-driven, practitioner-led program to create common vocabulary, standards, reusable data components, and tools that can reduce the design and development time needed to build and implement robust, agile information sharing capabilities. For government leaders, NIEM provides a foundation for building information sharing for more effective operations and greater efficiency and return on investment. For practitioners, NIEM provides the operational tools and proven methodologies to build and implement standards to enable real-time information sharing. For more information visit www.niem.gov.

3 Common Scenarios

When building or implementing a new CAD system, use case scenarios are very important during the requirements phase and can be the building blocks that provide a sound system foundation. These scenarios can be constructed based on present business processes that are to be continued, or future business processes and new ideas. At a minimum, use case scenarios for the PSDI project include:

- An Exchange Name or Description
- Communities of Interest
- Exchange Status
- Source
- Examples of Triggering Events
- Sample Scenario(s) Describing Real-World Events
- Sample Business Rules That Could Apply

To demonstrate how data interoperability is desirable, the PSDI Committee has identified a list of use case scenarios that provide real-world examples of data flowing into, and out of, CAD systems. An expansive list of use-case scenarios can be found in the document titled *Priority Data Exchanges for Local Communications Centers*. Examples of three use-case scenarios are listed below:

3.1 Scenario 1: Existing/Current

Burglar Alarm Activation: A suspect breaks into a house and the suspect's movement is detected by the premises alarm system motion detector. The premises alarm system signals the alarm monitoring company that a burglary has occurred at the premises. The alarm monitoring company operator transmits the burglar alarm data to the appropriate 9-1-1 Public Safety Answering Point (PSAP) via an electronic "exchange". The PSAP's CAD system processes the data as a new call-for-service. Police are dispatched, arrive, and investigate the crime. Please see the use case scenario "External Alarm Information" in the *Priority Data Exchanges for Local Communications Centers* document for complete details.

3.2 Scenario 2: Evolving

Multi-Media Info (Video, Photo, Audio): The communications center receives a photo of a child that is the subject of an Amber Alert. The photo has been stored on the CAD system. The photo is transmitted to all Mobile Data Computers (MDCs) in local police department vehicles as well as to other communications centers that have an interest in the matter. Please see the use case scenario "Multiple-Media Information into CAD (Video, Photo, Audio)" in the *Priority Data Exchanges for Local Communications Centers* document for complete details.

3.3 Scenario 3: Futuristic

Notification of Gunshot Location: The sound of gunshots is recorded, triangulated, and relayed to the appropriate PSAP via an electronic exchange. The PSAP's CAD system processes the data as a new call-for-service. Police are dispatched and investigate. Please see the use case scenario "Gunshot Location Event" in the *Priority Data Exchanges for Local Communications Centers* document for complete details.

3.4 Single Agency Environment

The communications center is the operational nerve center of the emergency service delivery system. It must be designed to prevent disruption of operations by internal and external events, including fire, natural and man-made disasters, and criminal or terrorist activity. An alternate or back-up communications center should be provided that, when fully staffed, is capable of performing the essential functions of the primary center. When a PSAP is not located within the communication center, it should meet the requirements for a communications center. Some examples of stand-alone communications centers that connect to other supporting centers are:

- A PSAP is the entry point for 9-1-1 calls and may hand the call over to an EMS communications or dispatch center.
- A Department of Transportation's Traffic Operations Center (TOC) has a communications center that interfaces with a PSAP.
- A federal installation may have a communications center that interfaces with the local PSAP.

Effective and reliable emergency communications systems play an essential part in the delivery of emergency services. In most cases, at least two independent communication paths, or circuits, should be provided for essential functions. These should be diversely arranged so that an event that damages one circuit is not likely to damage the other. Wire circuits (both metallic and fiber-optic) that are essential to the operation of a communications system must be well-maintained and should be monitored for integrity. In addition, essential systems must be able to operate during power failures. Therefore, uninterruptible power supply (UPS) backup power generators of adequate size should be provided both at communications centers and at remote sites. Remote site examples include a radio tower site, an alternate PSAP, or an emergency operations center (EOC) site.

Whether serving one or multiple political jurisdictions, one response agency or many, the communications center needs to be adequately staffed, during all hours of operation, to effectively receive and process emergency calls for service. Call takers and dispatchers, collectively called telecommunicators, provide the human interface between a person calling for help and the emergency service delivery system. They must be properly trained and familiar with the geographic area and agencies they serve. They need the ability to remain alert during periods of low call activity, and calm during periods of high stress.

Two-way voice radio is an essential part of emergency services communication. Radio systems must be carefully designed to provide complete coverage of the service area. A sufficient number of frequencies should be provided to handle anticipated peak radio traffic. Separate tactical frequencies should be provided for uninterrupted on-scene communication. Where radio is the primary means of dispatching, redundant radio base station transmitters should be provided. When used as a means of emergency dispatching, wireless paging systems should be under the direct control of the authority having jurisdiction (AHJ). The AHJ is the governing authority responsible for operating the center(s).

Rapid technological and social changes, including the proliferation of cellular telephones, increased emergency call volumes, increased demand for separate channels in a finite radio frequency spectrum, and expansion of intelligent transportation systems, will continue to challenge the managers of emergency centers and communication systems for many years to come. (Source: NFPA Fire Protection Handbook, 2008.)

3.5 Multiple Agency Environment

Multi-agency systems can touch on many areas. There are multi-agency radio systems, where one jurisdiction operates a trunked radio system for several departments. On a broader level, a region of multiple jurisdictions may operate a regional radio system that supports communications needs for each participating jurisdiction, several departments within each jurisdiction, and interoperability needs across the region by way of common radio talk-groups.

Some primary PSAPs often find the need to transfer a 9-1-1 caller to another primary PSAP. Primary PSAPs may also transfer 9-1-1 callers to a secondary PSAP. One example is when the primary PSAP answers a 9-1-1 call for emergency medical assistance but pre-arrival instructions must be provided by the EMS agency housed at a secondary PSAP. Another example is when the primary PSAP is located within one public safety agency (e.g., the police department) and all calls for the fire department must be transferred to a secondary PSAP.

The flow of data within any communications center is based on its organization, the number of agencies it supports, and any interfaces that may be in place. Ideally, all necessary data is captured by one CAD system at the primary PSAP level and disseminated internally (via radio, Intranet, pagers, MDCs, other internal agency CAD systems, etc.), then externally to other CAD systems as required. The need to exchange data within the multi-agency or multi-jurisdiction environment not only exists, but is becoming more important over time.

4 Common Information Flows: Originators and Recipients

Although there are variances based on jurisdiction and infrastructure, typical CAD data inputs originate from entities such as Automatic Number Identification–Automatic Location Identification (ANI/ALI) data, alarms and alarm companies, Geographic Information Systems (GIS), Records Management Systems (RMS), MDCs, various telematics, Intelligent Transportation Systems (ITS), and, of course, both landline and wireless calls.

Typical entities receiving outputs from CAD, again notwithstanding jurisdiction and infrastructure variances, would include other CAD systems, GIS systems, RMS systems, MDCs, ITS, fire stations, hospitals, fusion centers, and various disparate external databases.

Graphically, the environment could look like this:

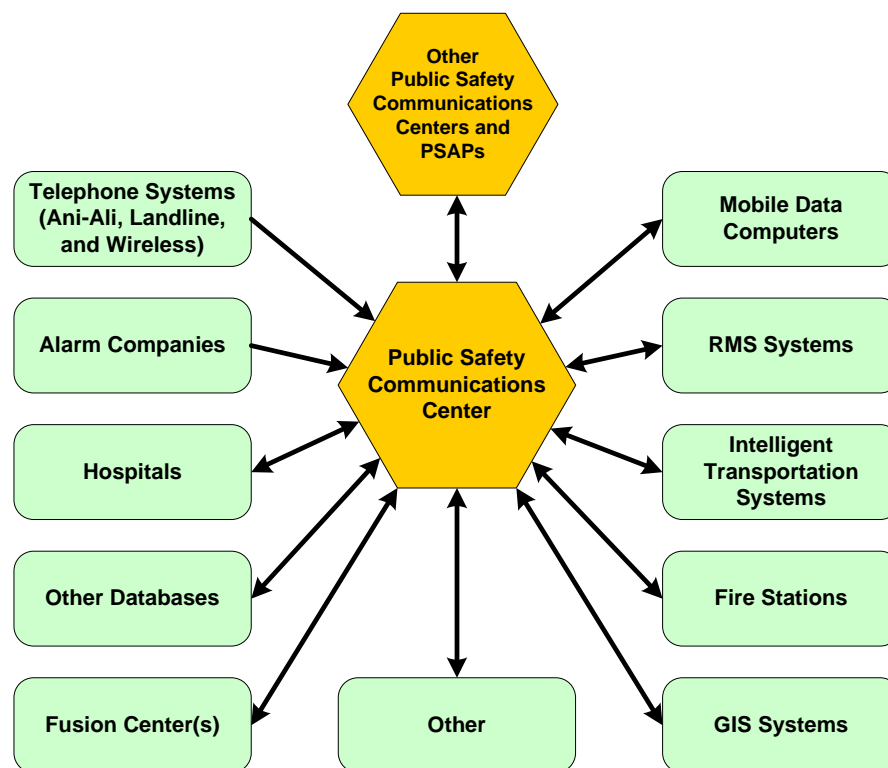


Figure 1

5 How is Data Interoperability Achieved?

5.1 Data Interoperability System Development – The Big Picture

Data interoperability, like voice communications interoperability, is a multi-component process that progresses in a public safety system from being mostly undeveloped through increasing levels of maturity. The process involves developing these components:

- Governance
- Standard Operating Procedures
- Technology
- Training and Exercises
- On-going and/or Regular Usage

At the highest level, the following SafeCom “Interoperability Continuum” describes the stages of a maturing system of interoperability as it progresses from left to right.

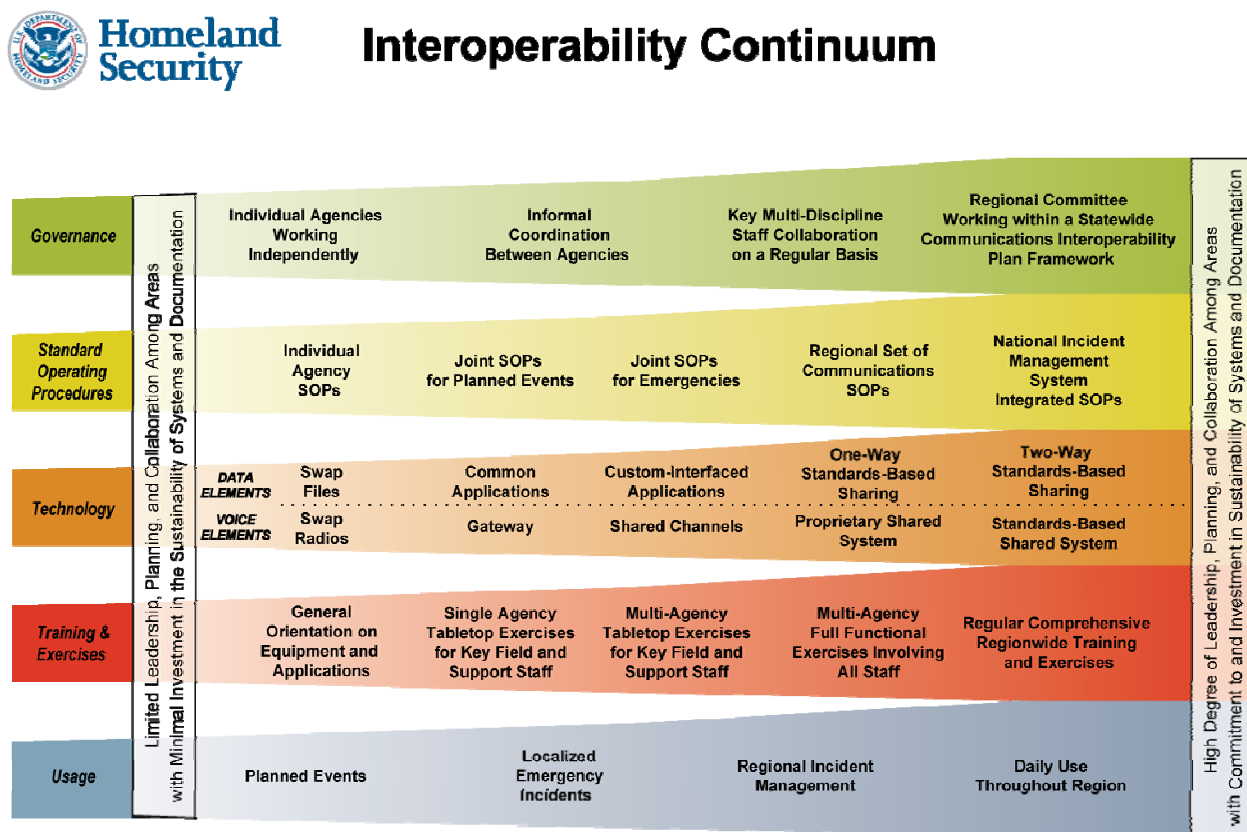


Figure 2

The only component in which voice and data communications are described differently is the technology component (or lane of the diagram). The specific increments from an undeveloped data interoperability system to a mature one are, per the SafeCom Interoperability Continuum brochure, as follows:

Swap Files — Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, emails, faxes). This process effectively creates a static “snapshot” of information in a given time period. Though swapping files requires minimal planning and training, it can become difficult to manage beyond one-to-one sharing. With data frequently changing, there may be issues concerning the age and synchronization of information, timing of exchanges, and version control of documents. Each of these issues can hinder real-time collaborative efforts. In addition, the method of sharing files across unprotected networks raises security concerns.

Common Applications — The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data. Common proprietary applications can increase access to information, improve user functionality, and permit real-time information sharing between agencies. However, the use of common proprietary applications requires strong governance to coordinate operations and maintenance among multiple independent agencies and users. These coordinated efforts are further compounded as the region expands and additional agencies use applications. Common proprietary applications also limit functionality choices as all participating agencies must use compatible applications.

Custom-Interfaced Applications — Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom, “one-off” links or a proprietary middleware application. As with common applications, this system can increase access to information, improve user functionality, and permit real-time information sharing among agencies. Improving upon common applications, this system allows agencies to choose their own application and control the functionality choices. However, if using one-to-one interfaces, the use of multiple applications requires custom-interfaces for each linked system. As the region grows and additional agencies participate, the required number of one-to-one links will grow significantly. Proprietary middleware applications allow for a more simplified regional expansion; however, all participants must invest in a single, “one-off” link to the middleware, including any state or Federal partners. Additionally, custom-interfaced applications typically require higher maintenance and upgrade costs. Changes to the functionality of linked systems often require changes to the interfaces as well.

One-Way, Standards-Based Sharing — One-way, standards-based sharing enables applications to “broadcast/push” or “receive/pull” information from disparate applications and data sources. This system enhances the real-time common operating picture and is established without direct access to the source data. This system can also support one-to-many relationships through standards-based middleware. However, because one-way, standards-based sharing is not interactive, it does not support real-time collaboration between agencies.

Two-Way, Standards-Based Sharing — Two-way, standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly. As with other solutions, a two-way approach can increase access to information, improve user functionality, and permit real-time collaborative information sharing between agencies. This form of sharing allows participating agencies to choose their own applications. Two-way, standards-based sharing does not face the same problems as other solutions because it can support many-to-many relationships through standards-based middleware. Building on the attributes of other solutions, this system is most effective in establishing interoperability.

5.2 Data Interoperability System Development – Implementation Methodology

This section explores the detail and realities of implementing interoperable systems. What seems to be curable with technological “black boxes” is not. Technology is relatively easy, but agreeing to share data is not. Agreeing on how and when to share data is not easy, nor is agreeing on who can access shared data and under what circumstances. Agreeing on how to interface between databases is not easy. And the list goes on.

The next several sections of this User Guide cover topics such as:

- Why data interoperability is so hard.
- The importance of a common standard.
- A real-world approach to data interoperability.
- Scoping an interoperability approach.
- Making it happen.
- Maintaining the effort.

These considerations are the detailed, real-life challenges involved in moving a data system from the left side (less interoperability) of the Interoperability Continuum to the right side (more interoperability).

There are many variables that factor into the successful implementation of data interoperability. Failing to address any one of these variables can completely undermine interoperability efforts. Some of the most important of these variables include:

5.2.1 Governance

There is no question that governance issues are the most challenging part of implementing data interoperability, especially if the data needs to be shared across both jurisdictional and discipline boundaries. The critical first step is to put in place a governance group of agency decision makers, as they will have the necessary “clout” to achieve the desired results. A Memorandum of Understanding (MOU) or similar agreement must be signed by all participating agencies. This stage of the process can be frustrating and time consuming, but it must be completed effectively.

5.2.2 Disparate Systems

The reality of the public safety world is that a significant number of agencies use proprietary systems that contain the information that needs to be shared. As new systems are specified, purchased, or built, agencies should be very sensitive to the need to conform to existing standards, which will enable the systems to exchange data easily and effectively.

5.2.3 Custom Interfaces

Proprietary systems have historically exchanged data using custom interfaces. In any new project, the viability of existing interfaces must be considered. It will be necessary, initially, to continue utilizing interfaces that cannot be replaced in a cost effective manner as a part of a new data interoperability project, but these custom interfaces should be replaced with standards-based interfaces as soon as practical.

5.2.4 Multiple Standards

Multiple standards have historically been a significant problem in data interoperability. Data standards such as eXtensible Markup Language (XML), the Global Justice XML Data Model (GJXDM), and the National Information Exchange Model (NIEM) have evolved to help remedy the interoperability issues between disparate systems. For public safety, the broad acceptance of the NEIM 2.0 standard for data exchanges will provide a basis for new data interoperability projects. Additional information about NIEM is provided in Section 2.3, NIEM and the Value of Information Sharing.

5.2.5 Lack of Funding

The shortage of appropriate funding continues to constrain local agencies which initiate the majority of the data sharing projects. An agency will need to creatively review all available funding options, including grants, bonds, and revenue sharing arrangements. It is important to remember that the funding source or program may drive the project approach and even the data exchanged.

5.2.6 Culture

Agency culture may represent one of the most vexing challenges to the implementation of data interoperability. Historically, agencies have built data “silos” based upon their unique needs without giving any consideration to the need to share data with other agencies. Even within organizations, different units have implemented “closed”, purpose-built systems under the guise of having “unique” requirements or of having “special” security needs. An example is the federal law enforcement community, where there are continuing struggles in the effort to change the culture from one of a “need to know” to one of a “need to share”. Cultural hurdles can quickly scuttle any type of data exchange process. Therefore, it is imperative that project planners and implementers set appropriate expectations with users and other stakeholders, and keep them involved at every stage of the project.

6 The PSDI Program Approach

The goal of the Public Safety Data Interoperability Program (PSDI) is to improve real time information sharing capabilities in the emergency response environment. Specifically, the PSDI Program seeks to promote the adoption and use of NIEM as the standard for sharing critical information between emergency communications centers, within and across jurisdictions, and between the Department of Justice (DOJ) and other relevant emergency management and intelligence domains of the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI).

Strategies to support this project goal are:

- Joining critical government, practitioner, industry, and stakeholder interests in the mission;
- Basing the solution on a national strategy for the application of information sharing standards;
- Producing a practitioner-driven solution to ensure critical business needs are met;
- Engaging the resources and expertise of industry to achieve technically-viable results; and
- Achieving “buy-in” through active and extensive stakeholder involvement.

The personnel resources for the project include a Project Committee comprised of 16 representatives from public safety communications, law enforcement, fire services, emergency medical services, emergency management, the public safety technology industry, DOJ’s Bureau of Justice Assistance (BJA), and the IJIS Institute. An IJIS Institute project manager, working in conjunction with a consultant representative from APCO, supports the committee.

Although future phases are expected, the current PSDI deliverables, other than this document, are:

- ***Priority Data Exchanges for Local Communications Centers*** – is a document for directors and other managers of public safety communications centers. Its aim is to provide an overview of many of the data exchanges that are of potential value to the communications center. Communications center directors and other planners may use this document to assess the current strengths, weaknesses, and growth potential of their facilities. In addition, the document provides a window into the future of data exchange in the communications center. Many of the exchanges described in this document are not yet in wide use, if at all. Directors and planners can use this information to understand emerging trends in data interoperability and to plan for future growth.
- **Information Exchange Package Documentation (IEPD)** – either new development or upgrades of existing high-value public safety data exchanges.

7 Important Technical Concepts

7.1 Information Exchange Package Documentation (IEPD)

To enable the reusability of local implementations, the concept of Information Exchange Package Documentation (IEPD) was defined and a methodology for their development was created. An IEPD is a collection of “artifacts” that support an implementer’s creation of an Information Exchange Package. This collection of IEPD artifacts gives implementers tangible products which can be leveraged for local implementation. Use of IEPDs has been proven to save time and money on interface development phases, from requirements to testing. Moreover, use of IEPD artifacts advances the widespread adoption of national standards as well as the realization of reuse benefits. For more information on IEPDs see the *NIEM Concept of Operations* document available on www.niem.gov.

7.2 The ANSI Process

As an American National Standards Institute (ANSI)-Accredited Standards Developer (ASD), APCO International is dedicated to ensuring public safety communications has a role in the development of standards that affect our domain. APCO’s standards development activities have a broad scope, ranging from the actual development of standards to the representation of public safety communications in other standards development areas. For a detailed description of the APCO ANSI process, we refer the reader to Appendix B.

8 Getting Started: a Real-World Approach to Data Interoperability

This section of the document discusses the following topics:

Scope Your Efforts – in this topic, we offer a detailed, formal process that communications center directors may use to evaluate potential data exchange projects. This process helps directors choose the projects that offer the highest business value to their organizations and communities.

Make it Happen – next, we discuss important aspects of project management for data exchange projects. These topics include funding, selection of business and technology partners, and issues regarding construction, testing, and deployment of exchanges.

Keep it Happening – finally, we discuss key issues regarding ongoing maintenance and management of data exchanges in a production environment. These issues include:

- Process improvement
- Adding additional business partners
- Evaluating IEPD enhancements
- Sharing lessons learned and best practices with your peers

Each of these topics is discussed in more detail below.

8.1 *Scope Your Efforts*

Before implementing any type of data exchange, the agencies involved must identify the business need(s) for it, as well as the business processes that support it. Once this is done, they can begin to define the data that needs to be exchanged. To assist in this effort, the PSDI Program created the *Priority Data Exchanges for Local Communications Centers* document to help identify exchanges of interest. Also included are use-case scenarios to aid in your decision-making. Once you have determined what information needs to be exchanged between your communications center and another entity/system, a prioritized list can be constructed. After the list is completed, interfaces for the data exchanges can be developed as funding and resources allow.

8.1.1 Determine Relevant Data Exchanges

The reader should review the exchange list and use-case scenarios in the *Priority Data Exchanges for Local Communications Centers* document, along with the exchanges listed in the IEPD Clearinghouse (see Appendix A) that have potential relevance to your potential data interoperability project. The *Priority Data Exchanges for Local Communications Centers* document includes a chart of identified CAD exchanges that could be used as a checklist for the PSAP – to check which ones are already in place, and which are needed/desired.

8.1.2 Map Relevant Data Exchanges on a Value Graph

After potentially relevant data exchanges are identified, they should be placed on a Value Graph. The Value Graph is shown below:

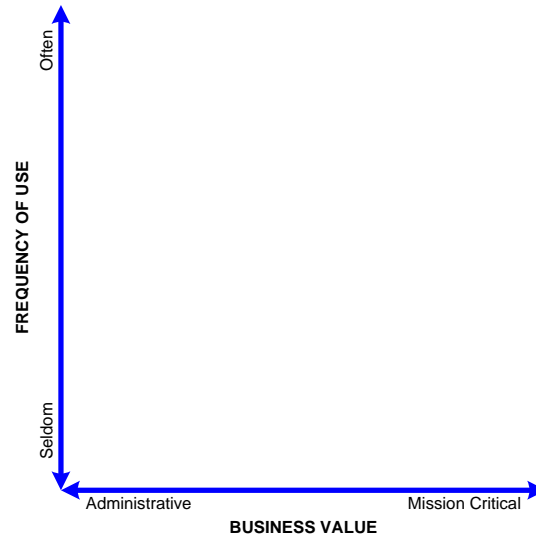


Figure 3

The horizontal axis is a range of Business Value, from Administrative processes to Mission Critical processes. The vertical axis is a range of Frequency of Use, from infrequent use to frequent use.

Each potential data exchange is mapped by the communications center manager or governance entity in terms of relative frequency of use and business value. Potential data exchanges are mapped on the graph as shown in the example below:

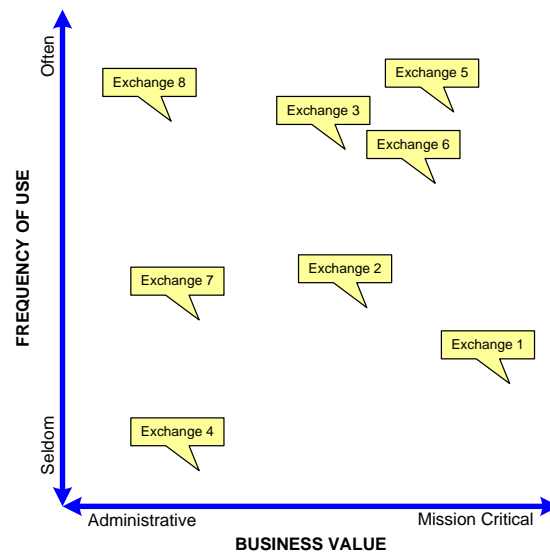


Figure 4

Select High-Value Data Exchanges: The map divides into four main quadrants that suggest different types of value propositions:

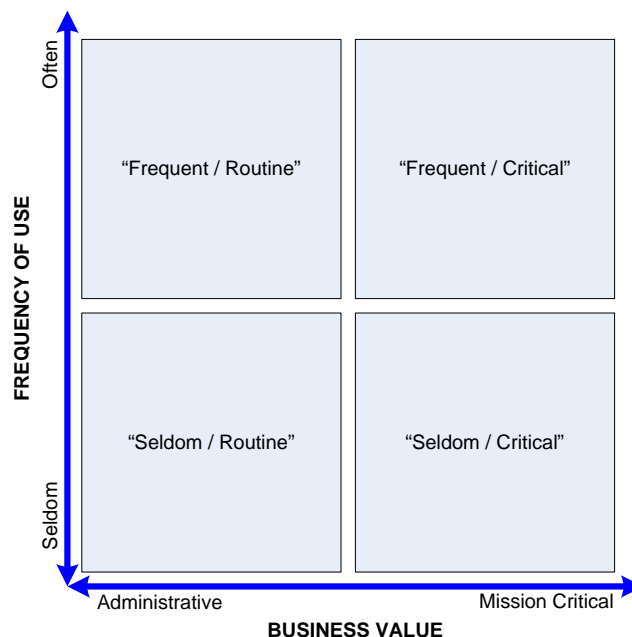


Figure 5

If an exchange will be used frequently, and also has mission-critical business value, it may be termed a **"Frequent/Critical"** exchange. It has very high potential for improving the operation of the Communications Center and its partners.

If an exchange is used frequently, but its value is more toward the Administrative side of the business value continuum, it may be termed a **"Frequent/Routine"** exchange. It has high potential to reduce costs for the Communications Center and its partners by automating common administrative business processes.

If an exchange has mission-critical business value, but is used infrequently, it may be termed a **"Seldom/Critical"** exchange. It might provide a high value capability in certain cases, but the cost of ownership will be high. In other words, it could be just as expensive to implement as a "Frequent/Critical" exchange (in terms of construction, documentation, training, etc.), but it will not provide sufficient Return-on-Investment (ROI) based on the frequency of use. In addition, since it is seldom used, it will probably require artificial exercises in order to keep all business partners up to speed on how to use the process. These exercises will also add to the cost of ownership. The Communications Center manager might choose to only develop this category of exchange if there is strong political motivation for doing so, for example.

If an exchange has only administrative value, and is also infrequently used, it may be termed a **"Seldom/Routine"** exchange. It is probably not a good use of resources (e.g., time, effort, personnel, funding) to implement such an exchange.

Mapped together the graph would look like this:

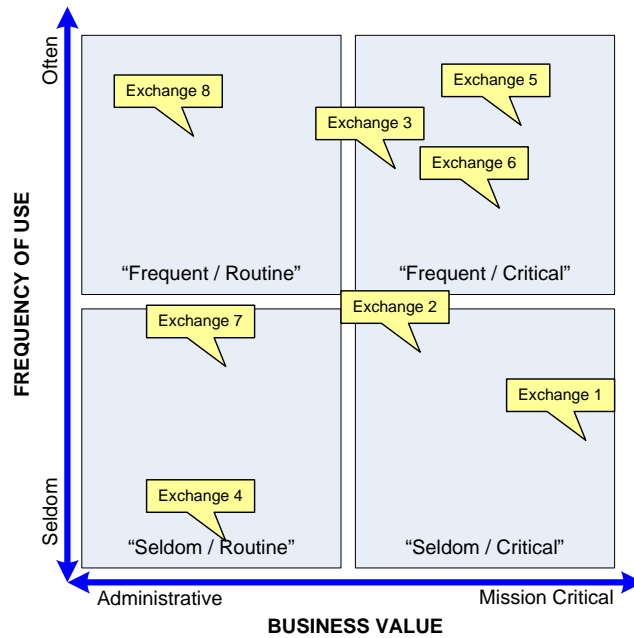


Figure 6

In this example, we can easily identify exchanges #3, 5, and 6 as, most likely, the highest priority exchanges.

9 Make it Happen!

9.1 Project Governance

Critical to the success of any IT project, particularly those that cross jurisdictional or agency boundaries, is the establishment and maintenance of a governance structure. No single governance model will meet the needs of all states' justice information systems integration initiatives.

NASCIO's Interoperability & Integration Committee recently published a research brief entitled *Connecting the Silos: Using Governance Models to Achieve Data Integration* (<https://www.nascio.org/nascioCommittees/interoperability/connectingSilos.pdf>). This brief attempts to answer questions such as, "What needs to be addressed when contemplating an information integration initiative, and what is being done in the states and at the federal level to develop information integration governance models?" It also includes other factors that are impacting governance in integration, offers references to models that have been used successfully by other states, and provides links to resources on information sharing.

9.1.1 Establishing a Governance Structure

A governance structure is an organizational body with the authority to make decisions and oversee the successful implementation of the project. A governance structure can take many forms. It can be formal or informal. There is no right way to establish one. The structure can be created using a variety of methods, including memoranda of understanding (MOUs) signed by partnering agencies and organizations within a collaborative effort; joint agreements signed by agencies in separate jurisdictions or by several government entities within a district or region; or through signed charters or other agreements. Whatever the method, a written statement of general goals should be prepared to identify the members and decision-making policies and procedures that are agreed upon in advance.

The governance document should also identify partners and participants, and it should identify everyone's roles and responsibilities. There also needs to be an understanding regarding the level of commitment of these individuals to the project. This helps avoid the potential of involving governance members who lack the commitment to devote the necessary time and resources to the effort. Without such a commitment, the effort has a high potential for failure.

A key objective of the governance structure is to make certain the goals of the project do not get weighed down in politics, procedures, and turf issues. A governance structure generates levels of agency equality, sets the direction for the effort, and moves it forward. The governing body can facilitate the participation of small agencies and jurisdictions that might otherwise lack the resources to participate in large agency collaborations. It is imperative that all participating agencies, organizations, jurisdictions, and regions make progress toward achieving the agreed-upon goals and objectives. However, to successfully accomplish this objective, the governance body must ensure that the appropriate staff is assigned to the teams handling the day-to-day work of the project.

Members of the governance body should represent all agencies and public safety disciplines, jurisdictions, and regions participating in the effort, regardless of size. Members can be representative of the user side of the effort and may also include elected and appointed officials, jurisdictional budget professionals, and others deemed essential to a successful implementation.

A lack of funding could potentially be a critical obstacle both in terms of the project itself, and also in terms of establishing and maintaining the governance effort.

9.1.2 Maintaining a Governance Structure

As the project evolves, the governance structure and its establishing document should be re-examined to ensure the needs of the effort remain current. Changes may be required to keep the project moving in the right direction, with the right oversight.

Elected and appointed government officials have major responsibilities in the development, implementation, and institutionalization of an effort. They can provide the voice of political leadership, help reduce turf issues, and assist in securing necessary funding; but, to do so, they need to understand the nature of the effort and be educated regarding its benefit to the community.

Also critical to the success of the effort is identifying a “champion”. This can be an elected or appointed government official or other leader in the community. This individual (or individuals) must possess the appropriate knowledge of what the effort is trying to accomplish, and he or she must be committed to seeing the project through to completion.

9.1.3 Additional Recommendations

A survey conducted by Public Technologies, Inc., identified several recommendations for establishing local governance structures that can facilitate the integration of justice information systems.¹

- Ensure equal involvement from all participating agencies. “Turf battles are viewed by many as an impediment to the integration of the necessary systems.” These issues can be minimized, if all organizations participating in the project work in a coordinated and collaborative manner that will instill project ownership.
- Identify and Obtain Funding. Not finding the necessary funds to plan, develop, implement, and support an IT initiative can prevent organizations and jurisdictions from attempting to develop an information sharing system. Costs associated with system replacement, upgrades, and maintenance for both software and hardware can be overwhelming, if not properly planned for and estimated prior to developing an RFP.
- Develop a strategic plan with realistic goals and objectives. Unwisely, some jurisdictions and agencies attempt to undertake a project without the benefit of serious, detailed planning. Planning takes time and thought, and in some cases the desire to move the effort forward overcomes the need to have a clear, thought out plan. This shortcut approach can result in project failure. Early planning and phased approaches help the project achieve small successes along the way to the ultimate goal. These successes keep the governance board and its members motivated and ensure the support of the community for the long term.
- Implement a sound communication plan. A key purpose of a governance structure is to facilitate communication between all participating agencies and organizations. Open and honest communication with stakeholders is critical. Therefore, it is important that a detailed communication plan be established. Such a plan helps participants stay in the loop, relieving

¹ IJIS Institute (2006). Pre-RFP Toolkit (second edition), www.ijis.org/_resources/Resources.

inevitable trust issues and agency concerns, particularly in cases where agencies or organizations are working together for the first time.

- Many efforts have failed because they did not have adequate support from all parties impacted by the project, especially from elected and appointed officials. Good leadership, governance, collaboration, and open, honest communication are critical to any successful integration effort.
- Finally, for additional information on governance, see the following publications:
 - The *1999 Statewide Governance Structure Survey* by the National Criminal Justice Association (NCJA).
 - A governance discussion is in the NCJA publication, *States' Governance Of Justice Information Systems Integration: Managing Decision-making In An Integrated Environment / Observations And Insights From The Field*.
 - The National Governors Association (NGA) discusses how justice systems integration can improve public safety, meet state and federal mandates, and provide leadership opportunities in *Improving Public Safety through Justice Information Sharing*.

9.2 Fund the Project

In addition to state and local budget appropriations, projects are often supported by federal funding. This section of the *User Guide* examines integrated justice funding available from various U.S. government sources.

9.2.1 Federal Funding

The federal government distributes billions of dollars each year to state and local agencies to support a broad array of crime control and prevention initiatives. Much of this funding can be used to support record management and justice information sharing systems.

9.2.2 Grants

Each year, the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS) administer sizeable budgets aimed at funding state and local governments. In fiscal year 2005 alone, the combined available funds from these agencies totaled over \$4 billion. Some of these funds can be used to support technology for justice agencies. Programs and allocations are susceptible to change each year, so the reader is encouraged to visit BJA's current funding opportunities at <http://www.ojp.gov/BJA/funding/current-opp.html> and DHS's Open for Business – Grants page at <http://www.dhs.gov/xopnbiz/grants/#1>.

Some examples of programs active as of the last update of this document are:

- Justice Assistance Grant (JAG).
- National Criminal History Improvement Program (NCHIP)
- Department of Homeland Security (DHS)

9.2.3 State Administering Agencies

Many OJP formula grants are awarded directly to state governments, which then set priorities and allocate funds within that state. For more information on how a state intends to distribute formula grant funds, contact the appropriate administering state agency. For each state, a list of grant points of contact is available at <http://www.ojp.usdoj.gov/saa/>.

9.2.4 Alternative Funding Approaches

In restrictive budget environments, innovative financing options are important to consider. Developing new relationships, leveraging resources, and developing new user fees are just a few ways to form new funding approaches to support justice information sharing. Creating these new avenues of support can be as simple as signing a MOU with a partner organization, and can be as complex as encouraging a state legislature to adopt a new fine or fee associated with the criminal justice process. This subsection explores some of these alternative funding approaches — leveraging investments, financing options, and other user fees — that may provide additional support for a justice information sharing effort.

Leveraging Investments

Current budgeted funds for integrated justice systems may not be sufficient to fund long-term efforts to achieve the ultimate integration vision. Budgeted funds can help address the cost factor when combined with reallocated sources of funds and new funding resources (including federal and private grants, leasing of infrastructure, and fees). The first step, however, is to look at innovative ways to cut the costs of implementing integrated justice systems.

- **Shared Systems.** Many public safety agencies use shared systems and resources instead of building independent systems. Technologies such as Web Services, eXtensible Markup Language (XML), and middleware make the sharing of information from disparate systems more affordable and easier to implement. Not only do shared systems support integration, but jurisdictions can save money by leveraging economies of scale in making expenditures. This is one of the reasons that Service Oriented Architecture (SOA) is becoming more popular, since one of its goals is to acquire and implement a service and then have more than one agency use it. Shared systems can be vertical, supporting information sharing between different levels of government, such as between cities, counties, tribes, states, and federal agencies. Alternatively, shared systems can be horizontal, where several agencies of the same type or at the same level of government share information, such as when multiple law enforcement agencies share investigative information. When multiple agencies, jurisdictions, or governmental levels share a system, costs of the new system can be reduced for each agency to the degree that the cost of infrastructure, fixed equipment, maintenance, and applications are shared.
- **Volume Pricing.** Lower pricing, especially for equipment and software packages, can be a byproduct of the higher volumes generated by a shared system or by group purchasing agreements. Smaller agencies can enjoy the benefits of having purchases combined with those of larger agencies to obtain volume discounts. Developing purchasing alliances or compacts is another method of lessening costs. In order to avoid agencies with similar needs duplicating each other's purchases, agencies and jurisdictions should investigate group purchasing arrangements available through their respective state agencies, the federal government, and public interest groups such as the National Association of Counties (NACo).

-
- **Use of Existing Infrastructure.** If a governmental entity owns infrastructure that can be used for the new system, or if commercially-available infrastructure can be found, significant cost reductions can be realized. The conversion of up-front capital costs to long-term leasing costs can be of great benefit. Depending on the leasing rate and how long the leased item is used, the cost of leasing can equal or even exceed the cost of purchase or development. A specific fiscal analysis must be conducted to determine which method makes sense.
 - **Shared Information.** Contacting other governmental units that have already contracted with prospective vendors can provide valuable information on the prices that a vendor has charged to others.

The best results maximize economies of scale, but balance the size and effort against diminishing return. Economies of scale can be realized by sharing resources among agencies and jurisdictions. However, depending on the leasing rate and other factors, leveraging these economies of scale through the participation of other agencies and jurisdictions may increase the difficulty of implementing solutions, and outweigh the benefits. One trend that would alleviate this problem is the establishment of centralized procurement agencies, particularly at the state level. These agencies, with differing levels of authority, can be responsible for reviewing current IT infrastructure, defining goals for future capabilities and technologies, establishing standards, and assisting with the procurement process across a jurisdiction. In this way, the establishment of an enterprise or services oriented architecture can be more easily and efficiently achieved.

Some useful references for centralized oversight and procurement agencies include:

- Virginia Information Technologies Agency (VITA) (www.vita.virginia.gov)
- Arizona's Government Information Technology Agency (GITA) (www.gita.state.az.us)
- New York City's Department of Information Technology and Telecommunications (DoITT) (www.nyc.gov/html/doitt/html/home/home.shtml)
- NASCIO (www.nascio.org)

Financing Options

Financing methods for integrated justice systems include lease purchase agreements, capital appropriations, and bond proceeds. A government entity can use more than one financing method to achieve full funding. It is important to remember that financing methods used to fund assets generally must match the life of the asset.

- **Existing Funds**
 - **Capital Appropriation.** Compared to long-term financing, capital appropriation is in the pay-as-you-go category. The funding comes from revenues that are collected from current year taxes and fees. The government entity sets aside the funds for capital projects that usually take less than ten years to repay. Capital appropriations also are used to reduce dependency on long-term financing.
 - **Bond Proceeds.** This long-term financing method can be used for purchases that average 20 years to repay. For instance, a government entity needing \$5 million for infrastructure could prepare a public bond issue. The government entity obtains the money right away and makes payments through a debt service.

- **Usage Fees**

- **User Fees.** Many agencies charge user fees based on the number of individuals within the participating agency who use the integrated justice system. This approach is particularly effective in funding long-term costs; however, charging user fees can present fiscal and psychological barriers for agencies considering joining the system.

- **Private Partnerships**

- **Lease Purchase Agreements, or Fee for Service.** With most jurisdictions facing shrinking budgets, the search for alternative financing methods that do not require large capital investments has led to fee-for-service, or lease purchase, agreements. A private company or source can build and own the system, leasing it back to a government entity for a charge that usually includes a maintenance agreement. Care must be taken to ensure that appropriate levels of management control are exercised to meet law enforcement and judicial regulations. Additionally, issues regarding ownership, availability, and sharing of data must be thoroughly resolved.
- **Public/Private Partnerships.** Look for opportunities to partner among government agencies (public/public partnerships) as well as private sector organizations (public/private partnerships). Partnering builds ownership and greatly assists in project planning and implementation.

- **New Taxes**

- **Revenue Enhancement.** Some state and local governments have adopted specific fees, increased existing fees, or diverted some of the revenues from existing fees to fund new IT initiatives.
- **Special Fees.** Funding for integrated justice can come from revenue collected from special fees, such as the enhanced 9-1-1 fee for both landline and wireless communications, or from additional fees charged to offenders through court proceedings.
- **Motor Vehicle Fees.** Some states have used either existing fees or increased fees on motor vehicle and boat transactions. Due to the large number of transactions, these fees can generate significant funds.
- **Gaming Fees.** Several states have gaming operations that generate significant sums of revenue. Dividing the existing revenue collected or increasing the amount of revenue collected can provide a significant source of funds, both in the short and long term.
- **Public Transaction Fees.** Another source of funding could be public access or public transaction fees. These fees are paid by individuals processing transactions remotely such as paying fines, tickets, obtaining arrest reports, warrant and bonding information, traffic accident reports, etc.

According to guidance published by the U.S. Department of Transportation on building public/public and public/private partnerships, partners don't necessarily have to contribute funding. Knowledge, services, equipment, and public relations support are examples of contributions that other partners can make.

Chambers of commerce, for example, may become formal project partners because they want to improve public safety and reduce traffic congestion to promote tourism and economic development.

Furthermore, some industry groups may be interested in assisting a jurisdiction with an IT project in order to test or further develop a new technology. While there is some risk to the agency in taking this approach, in many cases the firm offers its services to the jurisdiction at a significantly reduced or no cost.

It is important that partnering agreements are formalized in writing so that all parties are clear about project responsibilities, as well as the benefits of participation. Sometimes, when partners are not contributing financially to a project, the project responsibilities can be taken too casually. Drafting a partnership agreement in the form of a MOU can help create the team discipline necessary to get things done.

9.3 Your Project Team and Implementation

The selection of project implementation staff and technology partner(s) are critical to the success of your IT project. Team members typically fall into four broad categories: internal/agency staff; other agency staff; technology assistance partners; and private consultants/firms. Depending on the complexity and scope of your project, you may need to use a combination.

Internal/agency staff typically are assigned as available and appropriate to assist with things like data input, training (after attending a train-the-trainer course), and sometimes as the project manager.

Other agency staff refers to personnel assigned to the project from other agencies – an example being staff from other agencies to support a new regional CAD system project. This staff may fill roles such as agency liaison, data entry, and trainer.

Technology assistance partners are entities such as the IACP/LEITSC/TTAP, SAFECOM ICTAP, and BJA (via IJIS Institute, SEARCH, and IIR). These partners can assist with things such as project planning, RFP creation, and some assistance with implementations. These services are often federally funded and can be used free or at reduced cost. See Appendix F: Additional Resources for additional information.

Finally, most projects involve a **private consulting firm, technology integrator, and/or technology provider** (software and/or hardware). Consultants frequently assist with project planning, RFP creation and evaluation, and can act as project managers and/or agency liaisons. Technology integrators specialize in bringing multiple entities together – both software and hardware providers and multiple agencies – and frequently provide project management services. Software providers offer a huge variety of systems in multiple (broad) categories of CAD, Mobile Systems, RMS, Message Switches, interfaces, collaboration tools, etc. Additionally, most software providers offer project management services, setup, and training as part of their implementation services. Hardware providers supply items like servers, workstations, laptops, mobile terminals, firewalls, hubs, routers, etc.

The determination of specific assignments, like that of project manager (PM), will also vary depending on the project scope and complexity, anticipated time/effort requirements, knowledge, and skill set. Sometimes the project manager is an agency member, but often the PM is from a consulting firm or the technology provider. If the PM is from outside the agency, the agency will still need to assign a project liaison (for example, a contracting officer technical representative) to act as the main conduit between the PM and agency resources and to facilitate agency decision-making regarding the project.

See the *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, *A Guide for Executives, Managers and Technologists* for detailed information on determining the project team members as well as project implementation.

9.4 Selecting Solution Providers

Selecting a solution provider for your data interoperability project, or for an investment in a system from which you plan to share information, can be quite daunting since the data interoperability environment is not only just still maturing, but is constantly changing. Many solution providers may proffer blanket statements that their product is interoperable; many may even use such phrases as “GJXDM compliant” or “NIEM compliant”. It is critical to ask the right questions and conduct the proper research to see if the solution provider truly understands data interoperability and if the product is one that will easily facilitate the transfer of data. Below are some candidate questions to ask the solution provider, preferably as a part of a required response to a Request for Information (RFI) or Request for Proposal (RFP) process.

Note – Do not merely ask if the provider is NIEM conformant. These questions are designed to understand to what extent a provider’s product will be conformant.

STANDARDS

- How many GJXDM/NIEM conformant information exchanges has your company implemented?
- How many GJXDM/NIEM conformant IEPD's has your company written or helped write in the past three years?
- How many of your technical staff attends GJXDM/NIEM developer training courses?
- How many IEPD's that your company wrote or helped to create have been posted in the IEPD Clearinghouse?
- Do your (list appropriate modules) contain all of the data components defined in the N-DEx IEPD published and available through the IEPD clearinghouse? If not, specify gaps and state when you intend to fill the gaps in a normal release cycle.
- Does your system include all of the individual modules specified in the LEITSC functional standards for CAD and RMS as published on the LEITSC web site, including the interfaces to external systems contained therein? If not specify gaps between your current product and the LEITSC specifications.
- Does your company participate in any federal or state data standards or information sharing initiatives/efforts?

PAST PERFORMANCE/QUALITY OF SERVICE/REPUTATION

- Provide a comprehensive list of all customers for the specific CAD or RMS solution being offered and for any other CAD or RMS solution for at least the past five years. The list should indicate if the customer is using the specific CAD or RMS being offered.

-
- Identify the ten most recent law enforcement agency installations of your CAD or RMS and identify whether the system is the specific RMS solution being offered or a prior generation RMS and provide a contact person from each of those agencies.
 - Identify the five most recent law enforcement customers that have discontinued use of your CAD or RMS and a contact person from each of those agencies.

OTHER QUESTIONS

- How many years has the specific solution you are offering been available as a commercial product (not beta)?
- What revision is the specific solution you are offering currently in? If a new version or revision is currently being developed, what is the projected date of its availability on the market? Is there any initiative that will result in substantial changes to your current proposed solution within the next three years?
- What partnerships have you established with other solution providers for associated systems, such as CAD, RMS, Link Analysis, Data Mining, Crime Mapping, etc.

Responses to these questions will assist you in determining whether a potential solution will help you down the path of interoperability or confine you within a proprietary solution. Solution providers should be quite willing to provide you with the answers to each of these questions. Answering all the questions, in and of itself, does not particularly validate the solution being offered. It is merely a tool to help streamline the potential choices.

Once solutions have been narrowed down, a reasonable selection should only be made after a hands-on demonstration of the product (never an on-line demonstration) has taken place in which the buyer can go in and “look under the hood of the product”. During the demo, ask the provider to export exchanges in NIEM format. This is the part of the process where, if the agency is not familiar with NIEM, having an external subject matter expert or consultant is highly valuable.

Following these steps will help in establishing an open relationship with a solution provider that will equip your agency with the appropriate technology to facilitate exchanges and enhance the environment of interoperability.

9.5 Keep it Happening!

Finally, we discuss key issues regarding ongoing maintenance and management of data exchanges in a production environment. These issues include:

- Process improvement;
- Adding other business partners;
- Evaluating IEPD enhancements; and
- Sharing lessons learned and best practices with your peers.

The initial efforts involved in achieving data interoperability will certainly be the most time consuming and challenging in the process. As an agency successfully accomplishes the exchange of data, the

inclination may be to believe that the project is complete. However, the data interoperability project is now moving into a new phase. As is true of all successful automation projects, the upgrade and maintenance to the data exchanges will require regular reviews. The maintenance phase of data interoperability will require dedicated funding and a clear assignment of maintenance responsibilities.

As success stories develop through the sharing of data, these stories can be included in the funding requests for on-going maintenance and enhancement of the exchanges. The maintenance efforts should consider the need for a help desk for problems as they arise from the continued use of the data exchanges. Any change in the systems (software, hardware, networks) of any of the participating agencies may result in problem reports that must be resolved. Users will not be able to rely on the information that is being exchanged if problem reports are not dealt with effectively and quickly.

9.5.1 Improve Processes

In addition to insuring that the existing exchanges continue to function effectively, effective data exchanges require scheduled periodic reviews to identify ways to improve the process. These reviews should involve the actual users of the core systems that provide the initial data collection. The reviews should be structured in a manner that will encourage users to identify ways to collect and share data more effectively. Enhanced ROI should be a guiding principle during these reviews.

9.5.2 Cast a Wider Net

In addition to looking for ways to improve the data exchange process, the regularly scheduled reviews of the data interoperability process should seek to identify additional agencies with whom the data could be shared. Opening up a meeting to include other potential partners will often result in the identification of new exchanges that could/should be added to the existing exchange network. The objective should be to share as much data as effectively as possible. The challenge may be to coax reluctant agencies to understand the benefit of expanded exchanges with additional agencies.

9.5.3 Evaluate IEPD Enhancements

An on-going maintenance program for data exchanges must also consider updates to existing exchanges and IEPDs, as well as the creation of new exchanges and IEPDs. Often, the need for updates or for new exchanges will become apparent during the process of using a system. User Group meetings should be scheduled on a regular basis, which could be quarterly. An annual meeting should be a minimum. These regular meetings would provide a forum for users to share ideas for enhancements and improvements to the data exchanges that are being used. These meetings will also provide an opportunity to learn about any pending changes in reporting requirements or system changes that may impact the existing exchanges.

9.5.4 Share Experiences with Your Peers

The process of effectively sharing data electronically is a relatively new development in the mission of public safety and integrated justice. The more effectively we can share our experiences, the more progress will be made. An agency should be willing to share both the high points and the challenges of their experiences in establishing and maintaining interoperability. We can learn from both our successes and our failures.

10 Appendix A: IEPD Clearinghouse

The Information Exchange Package Documentation (IEPD) Clearinghouse provides information on a variety of IEPDs that have already been developed and submitted by individuals and organizations who have implemented the Global Justice XML Data Model (Global JXDM) and/or the National Information Exchange Model (NIEM). The Clearinghouse can be accessed at <http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1108>.

No registration is required to access this site.

The image below shows a screen shot of the IEPD Clearinghouse web site.

The screenshot displays the IEPD Clearinghouse website. At the top, there is a header for "Justice Information Sharing" from the "U.S. Department of Justice, Office of Justice Programs". Below this, the page is titled "IEPD Clearinghouse". A navigation bar includes links for "IEPD Clearinghouse Home", "Find IEPD Information", "Submit IEPD Information", and "My Stuff".

Search options are provided with three filters: "Search by Product" (set to "All"), "Search by Category" (set to "All"), and "Search by Keyword" (with a "Search" button and a "Phrases" checkbox). Below the search bar, it indicates "149 Answers Available".

	Title	Summary
1	Law Enforcement National Data Exchange (N- DEx) IEPD v. 1.0.1 [Based on version 1.0 of the National	The Law Enforcement National Data Exchange (N-DE specifications to share criminal justice information.
2	NIEM-conformant Missing Persons IEPDs for New York State's eJusticeNY Integrated Justice Portal	These documents establish NIEM-conformant IEPDs f
3	NIEM-conformant Wanted Persons IEPDs for New York State's eJusticeNY Integrated Justice Portal	These documents establish NIEM-conformant IEPDs f
4	Arrest/Incident IEPD	This is a reference document illustrating how the XMI Amber Alert schema is proposed as a baseline for dev of AMBER Alert information
5	Amber Alert IEPD	The Incident Reporting IEPD provides a model for ele and national partners, including statistical crime analy
6	Incident Reporting Reference IEPD	Traffic Citation IEPD is a reference document designe Citations.
7	Traffic Citation IEPD	Arrest Warrant IEPD is a reference document designe
8	Arrest Warrant IEPD	The Charging Document IEPD can be utilized for Crin documents are generally initiated from submission of
9	Charging Document	This IEPD reference document is designed to support Fusion Centers share Suspicious Activity Report (SAI
10	Updated - ISE SAR IEPD 1.1	The Law Enforcement National Data Exchange (N-DE specifications to share criminal justice information.
11	Law Enforcement National Data Exchange (N- DEx) Incident/Arrest Information Exchange Package Documen	This IEPD reference document is designed to support partners share suspicious activities or incidents. Tha
12	Updated - SAR for Local and State Entities IEPD v1.1	

11 Appendix B: APCO International American National Standards (ANS) Process

APCO partners with many organizations advocating mutual public safety interests to develop standards that advance and benefit public safety. Collaborative efforts provide opportunities to address all interests, ensuring the most effective results and positive outcomes. APCO is an ANSI-accredited Standards Developer (ASD) and must comply with the ANSI requirements for standards development. These requirements provide standards developers with a neutral venue for benchmarking their standards development process. The ANS process requires that access to the standards process has been made available to anyone directly or materially affected by the activity under development. Periodic reviews of the standard are scheduled to ensure that the standard is a "living" document. ANSI's approval of these standards further verifies that consensus has been achieved.

Consensus signifies the concurrence of more than a simple majority, but not necessarily unanimity. ANSI promotes three additional "cardinal principles" that further support the consensus process. These are due process, openness, and balance. Due process means that any person may participate by expressing a position and its basis, having that position considered, and appealing if adversely affected. This is done through the public review and comment period. Appeals only pertain to issues regarding the process itself, not the content. Due process allows for equity and fair play. Openness is defined as any materially affected and interested party has the opportunity to participate in the consensus process. APCO cannot require consensus body members to be APCO members. The third, the standards development activity should have a balance of interests and shall not be dominated by any single interest category. APCO has three interest categories within each consensus body: users, producers, and general interests. These representatives are from all regions and different organizations. If a balance does not exist, APCO will actively solicit members to create a balance.

The APCO ANS process can take anywhere from 4 - 18 months depending on the content of the standard. APCO uses the latest technology to help the process be as efficient and effective as possible, which is extremely important with how quickly public safety communications is evolving. The APCO ANS Process consists of four major steps: Project Initiation, Public Review & Comment Period, Consensus Balloting and Review.

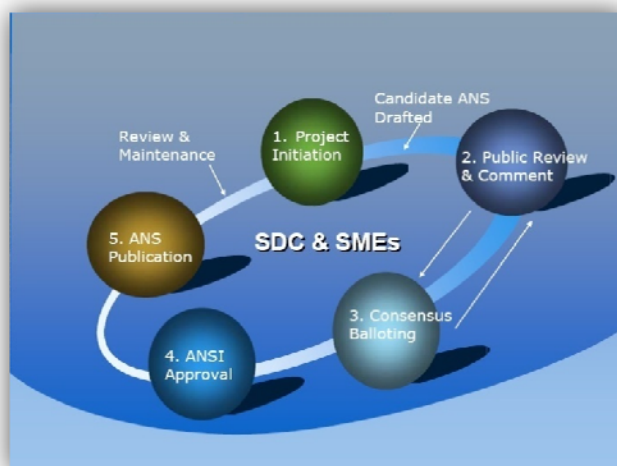


Figure 7

One of the initial steps is to publish the project initiation information within ANSI's Standards Action. This notifies other ASDs the project is in development with a description of the standard, as well as an explanation of the need for the standard. Once this is published, ASDs have the obligation to contact APCO if there is an existing standard that duplicates or conflicts with this project. If one exists, we must move forward with harmonization activities or withdrawal of the standard. This process allows for the document to become a candidate American National Standard, which once approved cannot be duplicated by other ASDs.

The next step in the process is the 45-day public review and comment period. At this time, any materially affected and interested party may review the document and submit comments on the candidate ANS. The preliminary document is made available for downloading on APCO's website which provides information regarding the type of comments that can be submitted and how to submit them. When comments are received, they will be sent to the workgroup or committee consisting of the subject-matter experts that developed the content of the candidate ANS for review and recommendations on how to respond to the comments.

APCO's Standards Development Committee (SDC) will respond to the commenter based on the recommendations. The SDC is comprised of a diverse group of practitioners who represent various public safety communications services throughout the nation. The SDC facilitates the APCO ANS process, working closely with the Subject Matter Experts (SMEs) who develop the content. We are obligated to respond to only relevant comments and those that provide potential solutions if they include a problem within the comment. If the subject-matter experts believe a substantive change is needed resulting from a comment, the change will be made to the document and the change will be subject to an additional 30 or 45 day public review and comment period.

Depending on the candidate ANS and the comments received, the consensus body will start its 15-day electronic balloting period, typically the last 15 days of the public review and comment period. If any negative votes are received, a relative comment and potential solution must be included. Once the balloting period has ended and if consensus was reached, the candidate ANS is submitted to ANSI's Board of Standards Review for final approval. When approval is received from ANSI, the document receives the finalized ANS designation with the approval year, an example would be "APCO ANS 3.102.1-2008."

APCO ANS Policies and Procedures require every ANS to be reviewed no later than four years for either reaffirmation, withdrawal, or any revisions needed. The APCO ANS process would begin again at that time. The ANS can be revised anytime before that if needed, keeping the standard relevant. Depending on what is decided during the development stages, a standard can be under continuous maintenance or periodic maintenance. With Continuous maintenance comments are accepted all the time and if comments are received that result in revisions or if the committee decides a revision is needed, only the revision will go through the APCO ANS process and a project initiation notice is not needed.

There is an appeal mechanism through ANSI, but it is only applicable for issues regarding the ANS process, not the content of the candidate ANS. The approved ANS must be published within six months of receiving approval from ANSI. APCO has been publishing its ANS on its website for complimentary downloading. For more information regarding the APCO ANS Process, APCO Standards Development Committee and/or APCO standards activities, please visit www.apcostandards.org or email standards@apco911.org.

12 Appendix C: NFPA Standards

In 2007, the National Fire Protection Association (NFPA) received a request from the Alliance for Public Safety comprised of several fire service and emergency organizations to establish a project and appoint a technical committee on fire and emergency service geographic information systems. The anticipated charge of the newly formed Technical Committee for Data Exchange for the Fire Service is to explore geospatial data needs and current applications and to develop common fire service standards and protocols for exchanging geospatial data among appropriate GIS user agencies and organizations during emergencies. This common exchange standard will benefit all fire service and other first responders in developing local, regional, and national security preparedness strategies and operations. The committee will develop a standard (or standards) that will assist all entities in achieving improved capabilities in planning resources for, and responding to, emergencies, whether the nature of the emergency is fire, medical, or natural or human caused disasters.

The NFPA process encourages public participation in the development of its codes and standards. All NFPA codes and standards (also referred to here as NFPA “Documents”) are revised and updated every three to five years in Revision Cycles that begin twice each year and that normally take approximately two years to complete. Each Revision Cycle proceeds according to a published schedule that includes final dates for all major events in the process. The process contains five basic steps leading to issuance of an NFPA Committee Document:

- Step 1 - Call for Proposals: Proposed new Document or new edition of an existing Document is entered into one of two yearly revision cycles, and a Call for Proposals is published.
- Step 2 - Report on Proposals (ROP): Committee or Panel meets to act on Proposals, to develop its own Proposals, and to prepare its Report. Committee votes by written ballot to approve its actions on the Proposals. If approval is not obtained, the Report returns to Committee. If approved, the Report on Proposals (ROP) is published for public review and comment.
- Step 3 - Report on Comments (ROC): Committee or Panel meets to act on Public Comments, to develop its own Comments, and to prepare its report. Committee votes by written ballot to approve its actions on the Comments. If approval is not obtained, the Report returns to Committee. If approved, the Report on Comments (ROC) is published for public review.
- Step 4 - Association Technical Meeting: Notices of intent to make a motion are filed, are reviewed, and valid motions are certified for presentation at the Association Technical Meeting. (“Consent Documents” bypass the Association Technical Meeting and proceed directly to the Standards Council for issuance.) NFPA membership meets each June at the Association Technical Meeting and acts on Technical Committee Reports (ROP and ROC) for Documents with “certified amending motions.” Technical Committee(s) and Panel(s) vote on any amendments to the Technical Committee Reports made by the NFPA membership at the Association Technical Meeting.
- Step 5 - Standards Council Issuance: Notification of intent to file an appeal to the Standards Council on Association action must be filed within 20 days of the Association Technical Meeting. Standards Council decides, based on all evidence, whether or not to issue the Document or to take other action.

13 Appendix D: PSDI Committee Members / Contact Information

13.1 PSDI Committee:

Ernie Blair

Director and CEO

Huntsville-Madison County 9-1-1 Center (Alabama)

(International Association of Emergency Managers (IAEM) representative)

MacNeil Cross

Chief (Ret)

New York City Fire Department

(Fire services representative)

Bill Kellett (Committee Chair)

Technology Architect

Microsoft

(IJIS Institute representative)

David Finchum

Law Enforcement Product Manager

BIO-key International

(IJIS Institute representative)

Wayne Gisler

Assistant Deputy Director

Traffic Engineering, Harris County Public Infrastructure Department (Houston, Texas)

(Transportation representative)

Alan Harker

Product Line Manager

Spillman Technologies

(IJIS Institute representative)

Linda Hill

Consultant

The Archer Group

(IJIS Institute representative)

Bill Hobgood

Systems Developer Lead

Department of Information Technology

City of Richmond, Virginia

(APCO representative)

Arthur Meacham

CAD System Manager
Caddo Parish Communications District (Louisiana)
(APCO representative)

Kevin McGinnis, MPS, EMT-P

Program Advisor, NAEMSO
(National Association of State EMS Officials (NAEMSO) representative)

David Mulholland

Commander
Information Technology & Communications
United States Park Police
(Law Enforcement representative)

James F. Slater III

Deputy Executive Director
Massachusetts Criminal History Systems Board
Criminal Justice Information Services Division
(Law Enforcement representative)

James Smalley

Manager
Wildland Fire Protection
(National Fire Protection Association (NFPA) representative)

Jonathan Spanos, PhD

Director
Customer Support/Interoperability
(National Emergency Management Association (NEMA) representative)

Barbara Thornburg

NENA Committee Resource Manager
(NENA representative)

Christopher Traver

Senior Policy Advisor
Bureau of Justice Assistance
(Sponsor representative)

Charles Werner

Chief
Charlottesville Fire Department (Virginia)
(International Association of Fire Chiefs (IAFC) representative)

13.2 Other Contributors

Amanda Byrd

Special Projects Manager
APCO International

Calvin Harvey

Assistant Administrator, Incident Management
Harris County TX Toll Road Authority (HCTRA)

Scott Parker

Senior Project Manager
IJIS Institute

Stephen J. Wisely

Interim Director
APCO International

13.3 Contact information

For more information about the APCO-IJIS PSDI Program or the PSDI Project, contact:

Scott Parker

Senior Project Manager
IJIS Institute
scott.parker@ijis.org
www.ijis.org

Stephen J. Wisely

Interim Director
APCO International
WiselyS@apco911.org
www.apcointl.org

14 Appendix E: The APCO/IJIS Institute Partnership

IJIS Institute and APCO established an Alliance Partnership for the purpose of jointly addressing the public safety data interoperability issue, and to seek resources and funding to advance this mission.

The IJIS Institute is a nonprofit corporation funded mostly through grants from DOJ's Office of Justice Programs, Bureau of Justice Assistance (BJA). The Institute uses these funds to assist "national scope" efforts related to information sharing in justice and public safety. The Institute comprises a membership of approximately 250 companies active in supplying information technology products and services to justice and public safety agencies. IJIS Institute achieves its mission of advancing information sharing through the development and endorsement of standards, and by providing assistance to local, tribal, and state agencies. The IJIS Institute was founded on the premise that information sharing is a significant national imperative and that a public/private partnership is the most effective way to achieve this goal. The Institute has developed and implemented a service delivery model that combines the best of government and industry. The model engages stakeholder organizations and practitioners, via committees, to ensure that business requirements are represented. The IJIS model also provides the best expertise to ensure solutions are viable. The IJIS Institute staff is comprised of professionals with over 100 years of collective experience in training, consultancy management, project management, and technical support. The IJIS Institute team is augmented by the expert resources of industry.



The Association of Public Safety Officials (APCO) International has a strong cadre of senior management executives, technical staff, and enthusiastic committee structure that is perfectly positioned to support the IJIS Institute and affiliated organizations to undertake and successfully complete the objectives of this project. APCO has a long history of providing leadership in a myriad of public safety projects and initiatives. Through the 70-plus-year history of APCO, it has been at the forefront of projects dedicated to the safeguarding of our citizens and improving public safety communications. APCO's qualified staff champions projects with goals to standardize processes, procedures, and services. After receiving its first federal grant award for the research and development of a public safety communications standard operating procedure manual, APCO has undertaken a variety of projects to enhance communications standards, notable examples of which are "Project 36" and "Project 38." Project 36 was initiated to research and develop universal standards for Computer Aided Dispatch (CAD) and CAD-to-CAD exchanges. The goal was to design effective processes for the exchange of data between third party call centers, such as alarm companies, and Public Safety Answering Points (PSAPs). The Project 36 activity was turned over to the APCO Data Transfer Committee and the work is on-going today. APCO and the Central Station Alarm Association (CSAA), in conjunction with outside vendors and two working PSAPs, have successfully demonstrated the initial objectives of the ALERTS Alarm Project. IJIS Institute, working with the aforementioned organizations, is assisting in the exploration of the additional beta sites. The work done in this arena illustrates the need to expand upon this initial demonstration activity. APCO, through its staff and committee partnerships, has within the last four years undertaken high profile nationwide projects, most notably, APCO "Project 38" (also known as Project LOCATE). APCO is an ANSI Standards Development Organization and in this capacity will be actively working with its Standards Development Organization (SDO) committee to move forward in the critical area of standards.



15 Appendix F: Additional Resources

15.1 JTTAC Training & Technical Assistance Opportunities

The Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), supports comprehensive training and technical assistance programs to advance the successful implementation of justice information sharing across the country. BJA coordinates the implementation of this training and technical assistance through a strategic partnership of national stakeholder organizations known collectively as the Justice Information Sharing Training and Technical Assistance Committee (JTTAC). JTTAC represents several organizations that play significant leadership roles assisting jurisdictions across the country needing training and technical assistance. It is through the collective efforts of the JTTAC members, combined with funding from BJA, that numerous courses and assistance opportunities are available to the field.

JTTAC resources are available at <http://www.it.ojp.gov/jttac>.

15.2 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.

Contact information—www.ijis.org

15.3 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**
- **Program Evaluation**

-
- Policy Analysis and Technical Training
 - General Training Workshops and Seminars

Contact information—www.iir.com

15.4 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. Its offerings include:

- Technical Assistance Program
- High-Tech Crime Training
- Justice Information Exchange Model (JIEM) Tool
- JIEM Training

Contact information—www.search.org

15.5 Law Enforcement Information Technology Standards Council (LEITSC)

LEITSC offers technical assistance to law enforcement agencies that are in the process of procuring or updating a Computer Aided Dispatch (CAD) system and/or a Records Management System (RMS). The technical assistance is driven by an agency's use of the Standard Functional Specifications for Law Enforcement CAD and/or RMS and is provided at no cost. Law enforcement agencies can leverage this opportunity when developing a request for proposal (RFP) for CAD systems or RMS. LEITSC has also made available the CAD/RMS Assessment Tool, which is designed to help agencies formulate RFPs for CAD and RMS systems. (www.leitsc.org/index.html)

15.6 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. (www.it.ojp.gov/global)

15.7 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. (www.llis.gov)

15.8 National Information Exchange Model (NIEM)

NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share

critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. (www.niem.org)

16 Appendix H: Glossary

AHJ	Agency Having Jurisdiction
ANI-ALI	Automatic Number Identification - Automatic Location Identification
ANS.....	American National Standard
ANSI.....	American National Standards Institute
APCO	Association of Public Safety Communications Officials International
ASD.....	Accredited Standards Developer
BJA.....	Bureau of Justice Assistance
CAD.....	Computer Aided Dispatch
CITA	Crime Identification Technology Act
COPS.....	Community Oriented Policing Services
CSAA.....	Central Station Alarm Association
DHS.....	Department of Homeland Security
DoITT	New York City's Department of Information Technology and Telecommunications
DOJ	Department of Justice
EMS	Emergency Medical Services
EOC.....	Emergency operations Center
GIS	Geographical Information System
GITA.....	Arizona's Government Information Technology Agency
GJXDM.....	Global Justice XML Data Model
GPS	Global Positioning System
HTML.....	HyperText Markup Language
IACP.....	International Association of Chiefs of Police
IAEM.....	International Association of Emergency Managers
IAFC	International Assoc of Fire Chiefs
ICTAP	Interoperable Communications Technical Assistance Program
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
IIR	Institute for Intergovernmental Research
IJIS	IJIS Institute
IT	Information Technology
ITS.....	Intelligent Transportation Systems
JAG	Justice Assistance Grant

LEITSC.....Law Enforcement Information Technology Standards Committee
LETPP.....Law Enforcement Terrorism Prevention Program
MDCMobile Data Computer
MOUMemorandum of Understanding
NACoNational Association of Counties
NAEMSO.....National Association of State EMS Officials
NASCIONational Association of State Chief Information Officers
NCHIPNational Criminal History Improvement Program
NCJANational Criminal Justice Association
NCJRSNational Criminal Justice Reference Service
NEMANational Emergency Management Association
NENANational Emergency Number Association
NFPA.....National Fire Protection Association
NG9-1-1.....Next Generation 9-1-1
NGANational Governors Association
NIEMNational Information Exchange Model
ODNI.....Office of the Director of National Intelligence
OSLGCP.....Office for State and Local Government Coordination and Preparedness
PSAPPublic Safety Answering Point
PSDIPublic Safety Data Interoperability
RFPRequest For Proposal
RMSRecords Management System
ROCReport on Comments
ROI.....Return On Investment
ROP.....Report on Proposals
SAFECOMa communications program of the Department of Homeland Security's Office for Interoperability and Compatibility
SDO.....Standards Development Organization
SEARCH.....The National Consortium for Justice Information and Statistics
SHSGP.....State Homeland Security Grant Program
SOA.....Service Oriented Architecture
TATechnology Assistance
TOC.....Traffic Operations Center (aka Traffic Management Center, TMC)

TTAPTechnology Technical Assistance Program
UASI.....Urban Area Security Initiative
VITA.....Virginia Information Technologies Agency
VoIPVoice over IP
XMLeXtensible Markup Language

17 Appendix I: Bibliography

IJIS Institute (2006). *Pre-RFP Toolkit (second edition)*, www.ijis.org/resources/Resources

National Association of State CIO's Interoperability & Integration Committee (2005). *Connecting the Silos: Using Governance Models to Achieve Data Integration*, www.nascio.org/publications

NIEM Program Management Office. *Requirements for a National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) Specification (Version 2.1)*, www.niem.gov

U.S. Department of Homeland Security (2008). *SAFECOM Interoperability Continuum*, www.safecomprogram.gov/SAFECOM/tools/continuum

U.S. Department of Justice, Office of Community Oriented Policing Services, Kelly J. Harris and William H. Romesburg (2002). *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, *A Guide for Executives, Managers and Technologists*, www.cops.usdoj.gov/ric/ResourceDetail.aspx?RID=243

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative (2007). *The Value of NIEM*, www.niem.gov

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (2001). *A Guide for Applying Information Technology in Law Enforcement* (NCJ 185934)

NFPA 72 National Fire Alarm Code. NFPA 72 covers the application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, fire warning equipment and emergency warning equipment, and their components.

NFPA 910 Standard Classifications for Incident Reporting and Fire Protection Data. This document describes and defines data elements and classifications used by many fire departments in the United States and other countries to describe fire damage potential and experience during incidents. It does not provide guidelines for a reporting system or related forms.

NFPA 1221 Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems. This standard shall cover the installation, performance, operation, and maintenance of public emergency services communications systems and facilities. 1.1.2 This standard shall not be used as a design specification manual or an instruction manual.