

Increasing Public Safety Data Sharing Interoperability

By Rehan Chawdry

Public safety constituents are using federal funds to plan and implement data sharing initiatives in order to have access to better information and improve the level of service they provide to their communities. Unfortunately, the lack of interoperability between agencies and their individual software applications is driving inefficiencies into projects, making them too costly to complete in needed timeframes. A different approach is needed to provide more flexibility while lowering costs and removing complexities from the data integration process.

This article describes a strategic approach to cross-agency data sharing that protects existing investments by separating the data integration tasks from the overall data management strategy. It describes an approach using open standards, industry expertise, pre-built interfaces and automation.

Data sharing is a critical component to public safety. But sharing information has been compromised by a lack of interoperability between law enforcement agencies and their software applications. This problem stems from entities running different vendor solutions, mostly built upon proprietary standards. In this environment, sharing data requires one-off custom development for each unique relationship, making the data sharing process time consuming, expensive and not viable as a long-term strategy.

National Information Exchange Model (NIEM)

After 9/11, the federal government placed a greater focus on sharing data and created the National Information Exchange Model (NIEM) to standardize data exchange within the public safety arena. Several federal agencies have already adopted the standard, and as NIEM compliance increasingly becomes a requirement for federal funding, it is

filtering through state, regional and local agencies at a rapid pace. With limited grant money, constituents are selective in how they spend these dollars. Data sharing with NIEM is at the top of the list for many because of the greater intelligence that can be quickly accessed through cross-jurisdictional data sharing.

This article describes the state of the data sharing market in public safety, outlines Sypherlink™'s proven approach to data integration, and presents the different environments in which the solution can be used.

Background

Data sharing initiatives in public safety have often been implemented based on methodologies driven from a target application's requirements. The implications of this approach meant that once an application provider was selected, all of the complexities involved in the data integration were oriented toward solving the needs of that particular providing vendor.

Constituency needs were typically more homogenous in the past—within a single county or group of counties, for example. A single vendor implementation approach, often the only approach available, was usually sufficient to solve the integration challenges in these situations. Once an investment was made for a given application, the high cost of integration meant that initiatives were typically locked into a single vendor's application.

As data sharing constituencies have grown in size, the need to recognize different agency requirements has grown as well. In today's environment, a single application may not solve all participants' needs.

A more strategic approach that protects the data integration investments made in data sharing initiatives begins by realizing that an application is only

one piece of a larger data management strategy. Data integration should be an independent process guided by open national standards, supporting multiple needs as opposed to being a by-product of a single application.

Data Integration Challenges

Regardless of the approach taken for data integration, challenges exist that jeopardize budgets, process efficiency and the ultimate success of data sharing initiatives. These include:

- **Reliance on domain experts for source and target systems:** In many agencies, data is scattered across applications, systems, desktops and physical locations. Domain experts are rarely available and documentation is scarce.
- **Critical discovery and mapping tasks are largely manual:** Due to the complexity of the environment described in the previous bullet, agencies have no choice but to tackle data discovery and mapping the old-fashioned way—manually.
- **Lack of re-usability and flexibility:** As each new target system is manually mapped, unfortunately little (if any) of the previous work done can be leveraged on remaining maps.
- **Vendor lock-in:** Traditionally, data integration projects have been completed with a single vendor application. Although this approach may be sufficient for a single entity in the short term, long-term flexibility suffers, and larger projects involving multiple agencies are difficult, if not impossible, to manage.
- **High cost of maintenance:** As systems change or are replaced, re-mapping is inevitable, thus compounding the time, cost and effort involved in maintaining data sharing initiatives.

Increasing public safety data sharing interoperability

continued

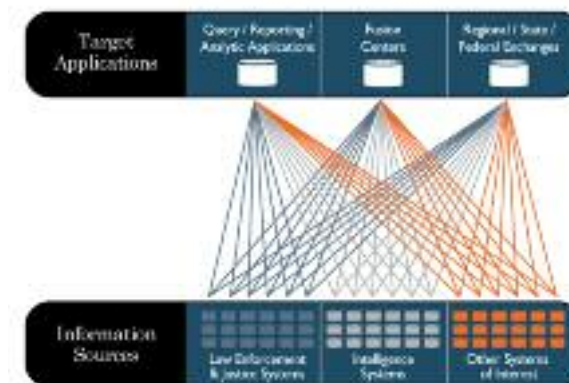


Figure 1: Point-to-point connections magnify the manual effort, cost and complexity of data sharing initiatives.

Integrated Justice Standards

The following sections outline the key standards developed by the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS) to be used in data sharing programs. Although NIEM/LEXS is becoming better understood within public safety, an overview of the origin, goals and challenges of the standards is necessary to understand the overall data integration picture as it relates to public safety.

NIEM Overview

NIEM is a joint effort of the DOJ and DHS, created as a means of effectively and efficiently sharing critical information at key decision points throughout justice, public safety, emergency and disaster management, intelligence and homeland security agencies. NIEM was designed to facilitate information exchange among federal, state, local and tribal agencies within the justice community.

To prevent the creation of domain silos, NIEM provides the framework, architecture, security and metadata controls necessary to guide the deployment of data sharing initiatives. It supports multiple domains and incorporates existing reference models, such as Global Justice XML Data Model (GXJDM), in its specification.

NIEM focuses on cross-domain information exchanges between key domains and communities of interest (COIs) across all levels of government—whether between individual local



Figure 2: NIEM domains.

law enforcement agencies, law enforcement and emergency service agencies, and other domains, or between local, state, tribal, regional and federal agencies.

Objectives

The main objective of NIEM is to promote coordination and synergies between disparate data sharing efforts. Through the use of reusability, it is designed to facilitate more cost-effective development and deployment of information systems; improved operations; better quality decision making as a result of more timely, accurate and complete information; and, as a consequence, enhanced public safety and homeland security.

The growing number of participants across the country benefit through faster time-to-value for strategic initiatives, lower cost of implementation and maintenance, reusable technology and knowledge, and greater access to funding and grant assistance.

The adoption of NIEM has also led to other important standards in the integrated justice community. LEXS provides a flexible, NIEM-based framework used for the creation of NIEM-conformant IEPDs for information sharing, both for publishing information and for system-to-system federated searches. LEXS specifies a set of schemas that establishes consistent definitions supporting publication, search and retrieval, both at a data level and a structural level.

Two basic categories of operations are defined by separate

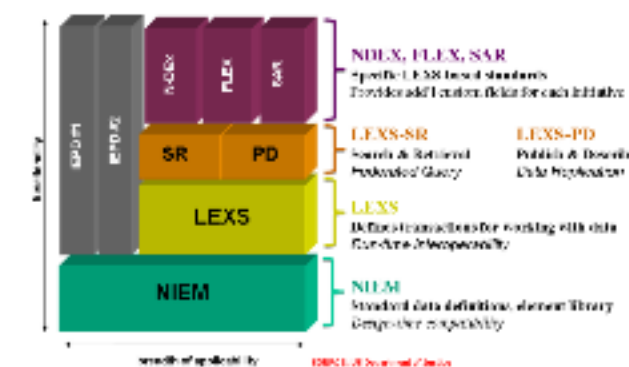


Figure 3: NIEM justice standards layers.

LEXS schemas, which are supported by shared schemas that provide common definitions of real-world objects and structures. LEXS Publish & Discover (LEXS-PD) is for publishing and updating data from a source to a consumer. It is currently used for data owners (or submitters) to publish to OneDOJ, N-DEx and other information sharing systems. LEXS Search & Retrieval (LEXS-SR) is for system-to-system federated searches and allows result drill-down to obtain more detailed information.

Integrated Justice Solutions

The above standards are building blocks developed by the U.S. DOJ and U.S. DHS in support of federal data sharing efforts. Individually, each solves a specific problem relevant to integrated justice, but together, they serve as a foundation for how data can be shared among different organizations irrespective of application, data or jurisdiction.

Increasing public safety data sharing interoperability continued

In the above diagram, the integrated justice initiative uses all of the building blocks to provide a NIEM-oriented data backbone that can interact with multiple sharing partners.

In some cases, individual agencies participating in an initiative may only contribute data from their law enforcement systems to a central data warehouse for some type of business intelligence. LEXS-PD provides a standard way to exchange this data, along with the necessary operations to support a warehouse-based approach.

In other cases, the initiative may seek to work with other integrated justice initiatives using a federated approach. In this scenario, all data stays within the boundaries of a given initiative but can be queried by an external party as necessary. LEXS-SR provides a standard way to support federated queries for this purpose.

Note that the above examples are independent of implementation architecture in the sense that NIEM and LEXS represent nothing more than data formats for an exchange.

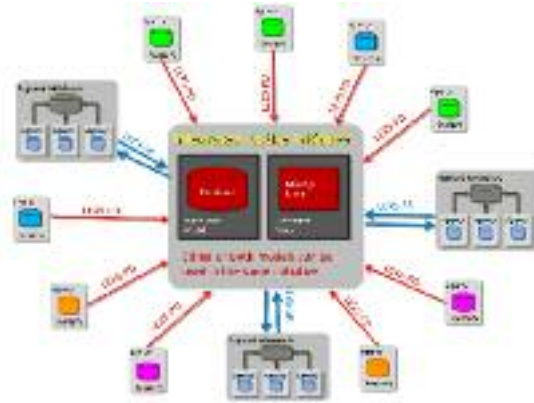


Figure 4: In the above diagram, the integrated justice initiative uses all of the above building blocks to provide a NIEM-oriented data backbone that can interact with multiple different sharing partners.

Solutions for Public Safety

It is important to implement data integration for public safety at both a tactical level, using execution components that can deliver data flexibly, and strategically, using federal standards as the data management backbone.

NIEM Architectures

The following section details how components described thus far can be used to solve key data integration challenges in the public safety environment. By comparing against traditional approaches, the integration architectures outlined below highlight some of the advantages of using a NIEM-based approach.

Data Warehouses

A number of initiatives, from state-wide data sharing efforts to DHS fusion centers, use a data warehouse approach to integrated justice functions. This approach seeks to copy data from end-point data sources into a central repository where sophisticated data analysis can take place. Warehouses tend to be used most often where deep analytics, crime patterns and other trend-oriented research is required. In integrated justice environments,

initiative sponsors such as fusion centers are not usually the owners of the data, including such entities as local law enforcement agencies. In these environments, traditional ETL, pull-based operations are complicated by the fact that the data owners typically want control of how their data is being used and will restrict access to external entities that require this data. As a result, push-based mechanisms that afford maximum control to the data owner are usually the preferred approach in these environments.

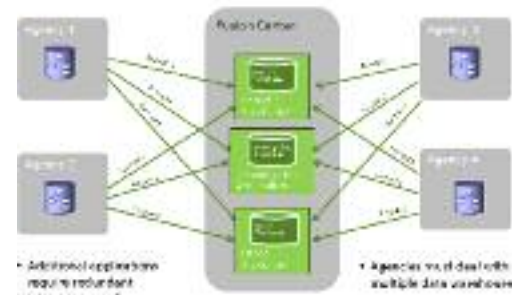


Figure 5: Traditional approach to integrated justice data warehouses.

The traditional approach fails to recognize the vendor landscape for end-point systems. More than 75 percent of public safety systems in use today are vendor-supplied. This industry comprises more than 300-400 different CAD/RMS, court, jail, emergency management, fire and other vendors that are often the source of data for most integrated justice initiatives. The vendors in this space have little strategic interest in adapting their data formats to other proprietary applications that would require development support from their respective organizations. These factors serve to increase the risk of most data warehouse projects. To address these shortcomings, NIEM-based integration components are suggested to isolate and manage the multiple data sources used in data warehousing initiatives.

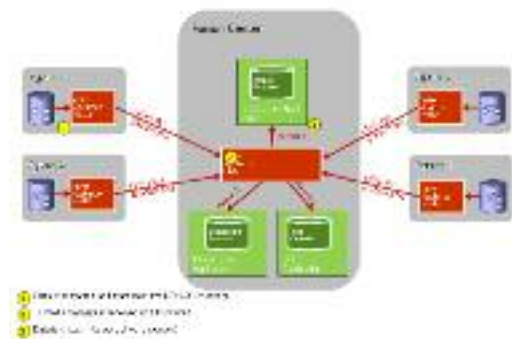


Figure 6: NIEM-based approach to integrated justice warehouses.

All data formats feeding the data warehouse are standardized to NIEM using the U.S. DOJ's LEXS Publish-Discover (PD) XML protocol. Software is configured to push data out at regular intervals as needed by both the project sponsor and the data owner.

Because the solution standardizes on a data format used nationally, vendors that have already written LEXS-PD adapters can be hooked into the solution with minimal to no work. At the central facility, the Hub ingests the LEXS-PD feeds from the different contributing systems and feeds them into one or more local warehouses for use by their respective applications.

Increasing public safety data sharing interoperability continued

Data Federation

The motivation for data federation architectures is to keep information where it currently resides but provide managed access to the underlying records for data consumers. One of the complexities in a real-world federation system is that query targets will often be systems implemented by different vendors and agencies, requiring a solution that effectively addresses the differences in schemas and architectures encountered in the problem space.

Simplified federation architectures make use of SQL-based methods to access underlying data records, meaning direct SQL calls are issued between requestor and end-point data source. At some point through the query chain, an initiating SQL query is translated to the schema of an end-point data source so the result set can be aggregated and interpreted consistently.

More recent federation architectures make use of an application level interface (API) that invokes SQL queries at a point closest to the data source.

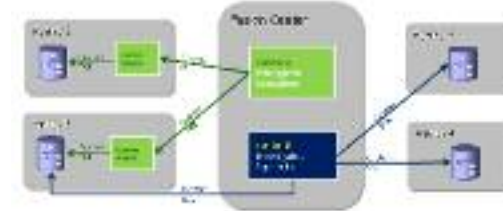


Figure 7: Traditional approach to federation in an integrated justice environment.

From an architectural standpoint, the API-based method provides a more manageable approach to data federation as a result of the separation between the requestor and the underlying distributed data schemas. A cleaner separation between these entities means external interfaces can be better localized. Using the components described above, a federation architecture using NIEM and LEXS can be deployed for use by any client application. Applications can invoke federated queries into the underlying LEXS-based subsystem.

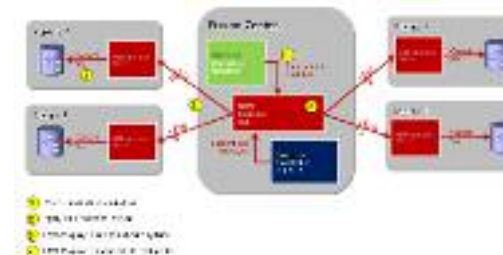


Figure 8: NIEM-based approach to federation in an integrated justice environment.

In addition, other systems that are LEXS-SR compliant can be interfaced without changes to the architecture. This allows the fusion center in the above example to interface to the FBI's N-DEX system, which uses LEXS-SR as a standard query mechanism into national law enforcement records.

Summary

The architecture and technology described in this article help constituents with varying requirements to increase flexibility, reduce costs, and shorten project timeframes while providing the assurance that funds will gain the highest possible return

at a time when they are difficult to attain. It is a combination of many factors that leads to these valuable results:

- **Out-of-the-box solution:** Such an application should include automation and pre-built interfaces to accelerate implementation and mapping. These technologies reduce resources and remove technical complexity from the data integration process.

- **Open standards support and expertise:** A decision to embrace NIEM/LEXS enables users to secure grant funding and promotes interoperability across initiatives. This in turn reduces training costs and shortens learning curves.

- **Strategic flexibility:** An open architecture protects investments made in existing standards, systems and infrastructure. This supports both physical and federated production models to meet the varying needs of its users and their partners. This also offers effective and cost-efficient change management as interfaces change, NIEM/LEXS models are updated, or standards evolve.

Conclusion

Today's integrated justice data sharing initiatives have evolved from single agency integration to multiple, heterogeneous constituencies with varying requirements. An implementation approach that provides for higher flexibility, lower costs, increased use of open standards and reduced timeframes is necessary to ensure that initiatives can continue to leverage the significant investments made to initially create them.

The approaches outlined in this paper provide a framework that can be used to strategically implement a data-sharing backbone. It emphasizes a vendor-neutral approach that supports the NIEM/LEXS standards, multiple connections, projects and initiatives while eliminating costly point-to-point connections.

By looking at data integration as a formal process as opposed to a by-product of any single application, an implementer is afforded the flexibility necessary to support data sharing initiatives both today and in the future.

Rehan Chawdry is an Integrated Justice/National Security Practice Leader with nearly a decade of experience in public safety and criminal justice. His extensive background in public safety information technology includes a comprehensive review and examination of data schema for more than two dozen law enforcement software programs. As practice leader for Sypherlink's National Security Practice, Chawdry is responsible for ensuring that the firm's information management solutions fully support the unique requirements of government agencies, as well as the new and evolving national data sharing standards, including the National Information Exchange Model (NIEM).

