

## USING TECHNOLOGY AND STANDARDS TO ENABLE CROSS-JURISDICTION SHARING OF CRIMINAL JUSTICE INFORMATION

### Abstract

This paper discusses the current state of criminal justice information integration, and how new standards and technologies are enabling new integration opportunities which allow law enforcement to provide greater local, state and national security.

### Keywords

SOA, NIEM, GFIPM, Service Oriented Architecture, JRA, Federated Identity, Web Services, CJIS.

### Introduction

Terrorist attacks and natural disasters in the United States have exposed weaknesses in our national, regional and local abilities to share government information. As a result, the Federal Government has made it a priority to improve information sharing in all areas of government to improve our abilities to detect, prevent, prepare, and respond to catastrophic events. The National Security Council has published a 'Strategy for Information Sharing' (2007) which sets forth the vision of the Administration on what improvements are needed and how they can be achieved. The Strategy states, "The exchange of information should be the rule, not the exception, in our efforts to combat the terrorist threat". This paper discusses some of the new standards and technologies that can further improve the sharing of information available from national, state, local and tribal government agencies. These same strategies can be used for integrating private and foreign partners as well. Currently, there are few criminal justice systems in operation that allow for the sharing and efficient exchange of state and especially local information. State, county, municipal and tribal agencies have a variety of existing heterogeneous systems in place. These systems often need to operate as a single integrated system in order to better serve the community. Today, most communication related to detailed information about people, places, things or events is done via telephone, fax or duplication of data. This leads to delays and inefficiencies in justice decision making, and limits the information available to law enforcement, prosecution, corrections and the courts.



# Whitepaper

*There is a demand for an integrated environment that enables efficient and effective justice data sharing.*

There is a demand for an integrated environment that enables efficient and effective justice data sharing. An integrated justice information system should bring new and enhanced capabilities, while leveraging existing systems as much as possible. Integrating these systems and sharing information within and between state, local and tribal agencies will lead to more effective law enforcement, better judicial decisions and ultimately safer communities. The sharing of information also brings about new requirements for safeguarding the privacy and improving the security of the data.

It is desired that the architecture of an integrated criminal justice information sharing system provides access to the required information on demand and in a useful form, regardless of the location of the data. The design should meet the scalability and availability needs of the system as it grows over time. But most of all, it should assure the security and privacy of the data that is now more readily available.

To meet these integration requirements, this paper presents some technologies and standards that are now being used in the criminal justice arena to promote system integration.

The Global Justice Information Sharing Initiative (GLOBAL) serves as a Federal Advisory Committee and advises the U.S. Attorney General on justice information sharing and integration initiatives. The organization promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete and accessible information in a secure and trusted environment.

GLOBAL has recommended the use of service oriented architecture (SOA) as a way to foster information sharing. GLOBAL has also recommended a federated identity model, which recognizes the GLOBAL Federated Identity and Privilege Management (GFIPM) framework as the recommended approach for the development of interoperable security functions for authentication and privilege management for sharing information across criminal justice information systems. Lastly, GLOBAL has been instrumental in the creation, adoption and deployment of a common extensible mark-up language (XML) data model to facilitate the exchange of justice information. Recently, the President has sent to Congress a declaration that the National Information Exchange Model (NIEM), which has extended the GLOBAL Justice XML Data Model (GJXDM) to other government domains, will be the common method for government agencies to share information.

# Whitepaper

These technologies and standards are enabling higher levels of integration between the nation's criminal justice information systems. The remainder of this paper will discuss some of the criminal justice integration challenges faced by governmental agencies and how these standards are employed to provide for better integration of today's criminal justice information systems.

## GLOBAL Justice Reference Architecture

### Integration Goals

The ability to achieve system integration between most existing criminal justice systems is limited due to their monolithic architecture. The majority of these systems were designed as centralized applications that run on one large server. Users typically use "dumb" terminals to gain access to the applications on the central server. As a result, they are centralized, closed and very controlled.

Other criminal justice information systems consist of departmental systems with personal computers connected to small servers. Some levels of integration are possible in this type of architecture, but information sharing is based on custom development of data transfer applications, using custom approaches for sharing information.

As a result, most of the systems participating in justice and law enforcement information sharing efforts provide custom interfaces, use custom means for integration, and have stand-alone "silos" of information which make it costly for sharing information.

The solution to this problem is to expose the data available in the silos utilizing standard methods of access and exchange such as Service Oriented Architecture.

### Description of Service Oriented Architecture

Conceptually, Service Oriented Architecture (SOA) is based on a distributed software model where application functionality is made available for use and integration with other applications over a network. A service provides a standard means for an application to expose its functionality. Other applications can use the service to access the functionality and data available from the application providing the service.

*GLOBAL's vision is stated as follows:  
"Any member of the justice community can access the information they need to do their job, at the time they need it, in a form that is useful, regardless of the location of the data."*



# Whitepaper

A service-oriented approach to the design and development of an information system assumes that basic components are developed to represent core functionality, and those components are combined into larger components, which can be loosely combined into even larger structures. This permits the evolutionary development of a system. Each component of this system exposes functionality that can be exposed to, and securely consumed by other systems as services. Service Oriented Architecture enables a model for integrating information systems regardless of the underlying technologies of those systems.

Existing systems need not be re-engineered to use the Service Oriented Architecture. A services layer can be added to each system that would allow for that system to expose functionality and data. For example, a service can be developed, which exposes certain business functions to its consumers. Internally, the service would be developed to natively communicate with the underlying system. Externally, all consumers of the service would have a common set of methods within the service that they would use in order to integrate with the underlying system.

The GLOBAL Advisory Committee (GAC) adopted a report on September 29, 2004, titled “A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)”, which was written by the GLOBAL Infrastructure/Standards Working Group. This report states the following:

- It recognizes Service Oriented Architecture as the recommended framework for development of justice information sharing systems;
- It adopts the report’s action agenda for its activities to further the utility of Service Oriented Architecture for the justice community; and,
- It urges the members of the justice community to take corollary steps in the development of their own systems.

The report states that GLOBAL’s approval of this report was based on the understanding that Service Oriented Architecture is an approach that is most likely to result in an infrastructure that will support its vision of how information should be shared among the justice community. GLOBAL’s vision is stated as follows:

*“Any member of the justice community can access the information they need to do their job, at the time they need it, in a form that is useful, regardless of the location of the data.”*

# Whitepaper

*SOA would allow the jurisdictions participating in the criminal justice integration effort to achieve higher levels of interoperability between new and existing systems.*

Service Oriented Architecture allows for placing components (services) which integrate with each of the existing systems and also provide for standards based integration between each of these systems.

SOA would allow the jurisdictions participating in the criminal justice integration effort to achieve higher levels of interoperability between new and existing systems. With the standards based implementation of SOA and the supporting infrastructure, it is finally possible to share information and meet the requirements stated by GLOBAL and the U.S. Attorney General's Office of Justice Programs.

This approach provides inherent scalability and can be utilized on multiple levels for local, state and state to state sharing of criminal justice information.

Service Oriented Architecture is based on the paradigm that providing systems can produce real-world effects which can be exposed via services to consumer systems. Thus a service is a mechanism to enable access to a set of one or more capabilities. A service is provided by one entity, the providing system, for use by others, the consumer systems. The reusability of the services approach is based on the fact that the provider may not be aware of the eventual consumers of the service and that the service may demonstrate uses beyond the scope originally conceived by the provider.

Service Oriented Architecture can be implemented as an orchestrated sequence of messaging, routing, processing, and transformation events capable of processing the exposed declarative properties of rich XML documents. The fundamental principles of Service Oriented Architecture are exposed functionality, document messaging, loose coupling, and platform independence. Existing systems can apply service oriented architecture to expose functionality to other systems by means of exchanging XML documents as messages. The usage of XML documents as the format of the messages helps provide the platform independence that is necessary given that there is a very wide variety of existing platforms represented in criminal justice information systems today.



# Whitepaper

The business processes of the state, local and tribal agencies participating in a cross-jurisdictional information sharing network could be exposed as web services, which would provide flexibility in the sense that these web services are reusable and pluggable. Another advantage of this architectural approach is that changes to business rules and processes can be made in the business layer, which results in minimal application layer changes and in many cases does not require development effort.

Along with GLOBAL's recommendation of service oriented architecture, they have developed the GLOBAL Justice Reference Architecture (JRA). The JRA provides guidance on implementing a service oriented approach to sharing information between justice and public safety applications. The JRA provides an integration strategy that is meant to prevent incompatibilities, facilitate communication and interoperability between agencies and will assist vendors and organizations in understanding how to develop solutions to meet these goals.

Additional information regarding the GLOBAL Justice Reference Architecture can be found at [http://it.ojp.gov/topic.jsp?topic\\_id=242](http://it.ojp.gov/topic.jsp?topic_id=242).

## Integration Benefits

Service oriented architecture is a promising strategy for integrating new and legacy criminal justice information systems. The addition of a service layer which exposes functionality of the underlying system to the consumers of the service has opened the doors to make it possible to access and share information between these critical safety applications.

Applications that were once stand-alone silos of information can now be connected. SOA enables the integration of these systems. Where in the past, integrating these systems meant custom development for each system, now utilizing Service Oriented Architecture allows a system to expose its functionality in a manner that is consumable by all other systems, greatly reducing the cost of integration.

While service oriented architecture provides a common model for connecting systems based on XML messaging, be it through web services, message queues, or other messaging technologies, there arises another integration problem.



# Whitepaper

The content of those messages must be standardized to continue to reduce the cost and complexity of integration. SOA does not define the content of the messages; the messages are tagged using XML, but there are no requirements for the structure and naming of the XML elements within the message.

To solve this problem of not having a common language to communicate the data elements between these integrated systems, a standard data dictionary, the National Information Exchange Model (NIEM), has been defined by the U.S. Department of Justice and U.S. Department of Homeland Security to provide standard definitions of the data elements within the messages.

## National Information Exchange Model (NIEM) Integration Goals

As stated earlier, terrorist attacks, hurricanes and organized criminal incidents have exposed the weaknesses that exist in our nation's information sharing infrastructure. The need for integration and information sharing is not limited to catastrophic situations: we need integrated information sharing in order to support the daily operations of public safety officials at all levels and across all branches of government.

Government and enterprise-wide information sharing is not universally possible today. While similar agencies capture common information and follow common business process, there are enough differences in the meaning and representation of the data that it makes it difficult to share information across agencies and jurisdictions in a timely manner. There hasn't been a national standard for representing the information that needs to be shared.

A large challenge in integrating data between one criminal justice organization and another is that each organization has different names and meanings for their data elements. Essentially, the criminal justice and public safety systems speak different languages. While they may be saying the same thing, they are using different words to represent similar data. For example, where one agency application uses the term 'arrestee', another agency application may use the term 'defendant' to represent the same person.



# Whitepaper

In order to improve integration between criminal justice organizations, there needs to be a common language, or vocabulary, that can be used by all organizations. This does not mean that all criminal justice applications need to be modified to use this common vocabulary, but rather use the common vocabulary while sharing information between applications.

To enhance the quality of government decision making, achieve greater efficiency, and accelerate information exchange design and development, there needs to be a common language that can be used as a standard for all information exchanges. The National Information Exchange Model was developed for these very purposes.

## Description of NIEM

The National Information Exchange Model is becoming the standard for sharing justice information. It was developed as a partnership between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS). The purpose of the NIEM is to enable jurisdictions to share information in the event of a national emergency and support the day-to-day operations of agencies throughout the country. The NIEM leverages the knowledge and experience gained in the process of development and adoption of the GJXDM.

The development of the GJXDM was funded by the Department of Justice (DOJ) and supported by the GLOBAL Advisory Committee (GAC). Agencies from all criminal justice domains and levels, federal, state and local, participated in the creation and enhancement of the model. GJXDM was developed to significantly advance justice information sharing by providing a common language and vocabulary.

The GJXDM is a large-scale, object-oriented data model with extensive inheritance, instantiated as XML schema; composed of reusable components and designed to facilitate disparate justice entities in exchanging information quickly, accurately, and reliably. It is a standards based data dictionary and reference model provided in the form of an XML Schema. The GJXDM can be used and further adapted by local, state and federal justice agencies to meet their specific domain requirements.

# Whitepaper

*According to the NIEM Program Management Office, “NIEM is designed to facilitate the development of enterprise-wide information exchange standards which can be uniformly developed, centrally maintained, quickly identified and discovered, and efficiently reused.”*

NIEM expands on the success of the GJXDM, which was focused solely on criminal justice, by extending it to include secure and timely information sharing across the broader justice, public safety, emergency and disaster management, intelligence and homeland security enterprise.

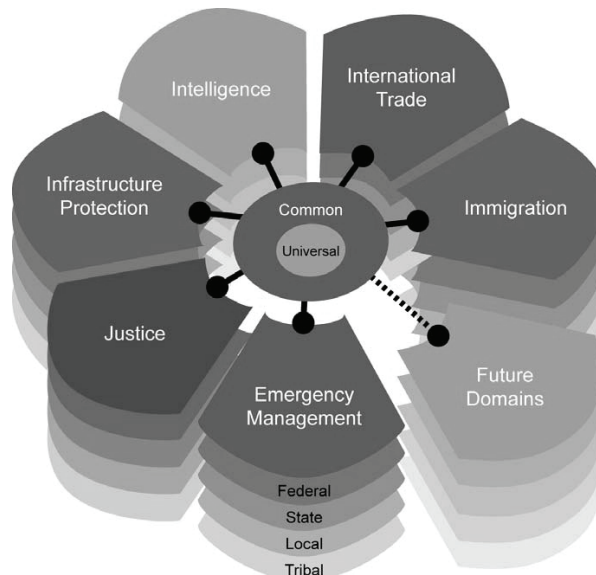
According to the NIEM Program Management Office, “NIEM is designed to facilitate the development of enterprise-wide information exchange standards which can be uniformly developed, centrally maintained, quickly identified and discovered, and efficiently reused.”

NIEM defines the data components that are the basic data elements that represent real world objects. These data components represent people, places, things and events. The definition of these components can be reused by practitioners when defining the information that is to be exchanged. NIEM uses XML schemas to provide for the consistent transmission of these components.

The NIEM is an intentionally large and inclusive data model and has defined the types of data components. Data components that are universally shared and understood (person, address, organization) across domains are referred to as Universal Components. These universal components represent the core attributes of a person, address, or organization.

Data components that are common across two or more domains are referred to as Common Components. Lastly, there are Domain Components that are specific only to a single domain, such as the justice domain, or the emergency management domain.

The following diagram is one view of the structure and hierarchy of the National Information Exchange Model.





# Whitepaper

The diagram demonstrates that the universal and common components that make up the NIEM core are available to each of the domains in the model. It also represents the fact that each domain can have components that are specific to their jurisdiction (Federal, State, Local, Tribal).

The NIEM is an overly inclusive and at the same time generic model. This leads to the need of exchange schemas which include subsets of the model and any extensions specific to the exchange that is modeled. Not all of the data elements available in NIEM are shared when specific information is exchanged between systems. For example, an arrest warrant can be represented using components of the NIEM model but when sharing arrest warrant information, the content of the message will only contain components that relate to an arrest warrant. This subset of the NIEM for warrants is called an Information Exchange Package.

An Information Exchange Package (IEP) is designed to further facilitate the use of the NIEM by building relationships between the data. This leads to increasing the value of the information exchanged, facilitates common understanding and enhanced usability.

The Information Exchange Package Documentation (IEPD) is a collection of artifacts that describe the structure and content of an IEP. The schemas and documentation in the IEPD is what is used and agreed upon by the agencies that are sharing information. This documentation defines the NIEM data elements that will be present in the information that is being exchanged, allowing both agencies to agree upon and use the content of the data within the message.

For additional information on the National Information Exchange Model (NIEM) please visit [www.niem.gov](http://www.niem.gov). Information on the currently published list of Information Exchange Package Documents is available at <http://it.ojp.gov/iepd/>.

## Integration Benefits

To effectively exchange information, there must be a common understanding of the data that is being shared between agencies, and that data must have a consistent structure. Agencies do not need to completely modify their existing information systems, but they do need to modify how they represent the data that is being exchanged.



# Whitepaper

According to the NIEM Project Management Office the expected result of standardizing criminal justice information exchanges on the NIEM is that there will be a far more efficient and expansive sharing of information between agencies and jurisdictions, more cost-effective development and deployment of information systems, better quality decision making as a result of more timely, accurate, and comprehensive information and tangible improvements in public safety and homeland security.

By providing a 'language' which defines the common naming and definitions for data elements, NIEM has provided a standard for how to represent the data in the process of sharing of criminal justice information. This common data model increases the ability for information sharing and level of integration between criminal justice information systems.

The combination of the GLOBAL Justice Reference Architecture and the National Information Exchange Model provide the 'how' and the 'what' for integrating criminal justice systems. However, as it now becomes easier to share information on a much broader scale, there needs to be a complementary focus on the security and privacy of that information. This leads to the 'who' of integrating criminal justice information: the GLOBAL Federated Identity and Privilege Management (GFIPM) framework.

## GLOBAL Federated Identity and Privilege Management (GFIPM)

### Integration Goals

Just as most criminal justice applications exist as standalone silos of data, so do the user identities for those applications. Each application has its own user store, forcing users to remember several user names and passwords in order to gain access to each application that they are allowed to use.

This situation usually leads to greater security challenges, such as passwords being written down or using the same password across systems to reduce the number of passwords that must be remembered. This can lead to a greater possibility that someone could obtain this information and wrongfully gain access to applications which contain highly sensitive and confidential data.



# Whitepaper

The multiple user accounts for each user also lead to a greater cost for the information technology (IT) department in that they have to manage all of these accounts. When a new employee is added, a user account needs to be created for that person in each of the systems that the new user has permission to access. And worse still, when an employee leaves an agency, the IT department needs to implement a process to remove this user from each of those systems; otherwise that user may still be able to gain access.

Today we are seeing many agencies making the move to have a single user store, usually a directory service based on Lightweight Directory Access Protocol (LDAP) or Microsoft's Active Directory. This moves the user identities out of each stand alone application, and into a central network directory service, which greatly simplifies user identity management. Now applications can be modified to rely on the central directory for user authentication. This consolidation of user identities, and the integration of applications with the central directory, means the user now only has a single user name and password to remember.

The problem still exists however. The central directory service put in place by an agency, or a county, only serves that agency or county. It is common that a law enforcement officer needs to access information available in systems provided by other counties, or by state and federal level agencies. To do so, they will still need to have user names and passwords for each of these county, state, and federal level systems. This not only leads to a user having multiple identities that they still need to remember, but also causes management and operational overhead for the provisioning of all of these identities.

It is unreasonable to have a single state-wide directory service to maintain user identities for all of the criminal justice users within a state. So there needs to be another means of integrating user identities across all of these systems. This is where identity federation and the GFIPM framework can be used to integrate user identities across system security boundaries.

## Description of GFIPM

The GLOBAL Federated Identity and Privilege Management framework provides a standards-based approach for implementing federated identity.

# Whitepaper

*A federated identity is an identity in one system that is securely authorized to access another system.*

A federated identity is an identity in one system that is securely authorized to access another system. The system that is providing a service or a web application is configured to trust user identities provided by another system.

The GFIPM metadata provides an understood, standard, definition of metadata across federation systems. This allows federated systems to have a common way to represent and communicate a user's identity and privileges, thus allowing system authentication and authorization decisions based on this standardized set of credentials. It is this concept of globally understood metadata across federation systems that enables interoperability and provides for the integration of criminal justice applications at the user level.

The GFIPM metadata is represented in XML and is conformant to the NIEM data model. A standard set of data elements and attributes represent information about a user, and about that user's privileges. Contained within the data elements is information about who the end user is, and how they were authenticated. The GFIPM metadata also contains information about the user's certifications, job functions, clearances, organizational affiliations, and any local privileges that the user may have.

To create a federated trust which allows remote user access to locally configured applications, an interaction between three critical components, a Service Provider, an Identity Provider, and the user credential assertions (GFIPM Metadata), is required. Within a federation, organizations will play the role of either a Service Provider, Identity Provider, or both.

The Identity Provider is the authoritative entity responsible for authentication and for providing the credentials of a user. It is the Identity Provider that asserts the identity for a user in secure fashion between the trusted partners in a federation.

A Service Provider is a federation partner who provides access to services, like web applications or web services. The Service Provider relies on the Identity Provider to provide claims or assertions about the federated user, and controls access to the managed services based on the trusted set of user credentials.



# Whitepaper

To make an agency application, such as a criminal justice web portal, accessible to trusted users, the application must be configured to be controlled by the Service Provider. The Service Provider must also be configured with the information about the Identity Providers that it trusts to provide user information.

An Identity Provider needs to be configured to access the local user store, typically Active Directory or an LDAP repository, of the trusted user and to build the GFIPM security token from the user's credentials and return that encrypted information to the service provider upon request.

When a locally authenticated user attempts to access a remote system, he or she no longer needs to sign on to that remote system. Rather, the Service Provider for that application will contact the Identity Provider for that user to get the user's credentials. It will then make authentication and authorization decisions to grant or deny access to the requested application.

## Integration Benefits

The benefit of a federated identity approach to security is that criminal justice application usage can now be expanded across jurisdiction boundaries without having to create duplicate user accounts for each application. This provides for greater integration of law enforcement knowledge because it enables secure access to larger amounts of information.

With the GFIPM framework defining a standard set of metadata representing a user's identity and their privileges, a trusting system can safely and securely provide information to a trusted user. This trusting, or integration, of user accounts across system boundaries provides for controlled access to a much greater set of criminal justice information than was previously available. Now an analyst, who was limited to searching their own systems and perhaps state and federal systems, can also securely access the systems of other integrated agencies.

By integrating user accounts across trusted systems, GFIPM, Federated Identity, and single sign-on solutions are greatly reducing the infrastructure burden of user account provisioning and management. Now, when creating a trust relationship between two agencies, all that needs to be done is configure the relationship that specifies that this agency trusts the other agencies users, and that the GFIPM credentials of the trusted users will be used to authorize access to the trusting system.



# Whitepaper

Individual user accounts no longer need to be created in the partner agency system in order to allow access to the partner application.

This user identity integration significantly improves the security of the shared information because with federated security, the home, or local agency is the only place responsible for the management of the user accounts. The integration, or consolidation of user account management down to having just a single user account at the place of employment, leads to increased cost efficiency and at the same time enhanced security of criminal justice applications.

## Conclusion

The National Criminal Intelligence Sharing Plan (NCISP), which was developed by the GLOBAL Intelligence Working Group and endorsed by the U.S. Department of Justice (DOJ), describes the information sharing requirements needed at all levels of law enforcement in this country. The plan identifies policies, guidelines and methods for developing and sharing critical data. Two real-world examples of the impact of the NCISP are the creation of Fusion Centers nationwide and the multi-state CONNECT project.

Fusion Centers have been, and are being, created in many jurisdictions to serve as a central and authoritative resource for the collection and exchange of information and intelligence. A Fusion Center provides a mechanism where law enforcement, public safety, and private partners can share and access information for the purpose of improving our homeland security and preventing criminal activity.

The CONNECT Project is a multi-state effort to effectively and securely share information, as specified by the NCISP, among the CONNECT member states. This project uses each of the technologies and standards identified in this paper. The GLOBAL Justice Reference Architecture is used to provide the integration of the variety of heterogeneous systems that exist in each of the states. The NIEM is used to define the standard messages that will be shared between the states, and the GFIPM framework will provide secure, federated access for the CONNECT project.

# Whitepaper

Fusion Centers and the CONNECT Project are just two examples of how the criminal justice community has benefited from new standards and new technologies which have provided for greater system integration, data integration, and user integration.

The GLOBAL Justice Reference Architecture, based upon Service Oriented Architecture principles, has allowed the justice community a means for integrating new and existing criminal justice systems. By providing a service layer in front of a justice application, other agencies are able to access and integrate the application into their own systems, thus providing greater capabilities to the user, as well as making far more information available than ever before.

The National Information Exchange Model (NIEM) has allowed the justice community to speak a common language in order to effectively share information. This standard means of representing criminal justice and public safety data has given the criminal justice community the ability to integrate data from other systems and sources that was burdensome or even not possible in the past.

The GLOBAL Federated Identity and Privilege Management (GFIPM) metadata and framework has benefited the members and partners of the justice community by allowing them to share information in a new way, with reduced management burden, and improved security. Federated security represents a strategic change in the way justice organizations establish the electronic trust that is necessary to share criminal justice information. GFIPM has provided a way to integrate the users of the criminal justice community.

The benefits of these new standards and technologies have allowed criminal justice applications, which had been stand-alone, inaccessible silos of information, to become highly integrated sources of information. It is this integration provided by these standards and technologies that has given law enforcement a far better ability to do their primary job, which is providing for the protection and safety of our nation.

*The benefits of these new standards and technologies have allowed criminal justice applications, which had been stand-alone, inaccessible silos of information, to become highly integrated sources of information.*

# Whitepaper

## References

National Security Council (2007)

National Strategy for Information Sharing [Online]

Available:

<http://www.whitehouse.gov/nsc/infosharing/index.html>

Global Infrastructure/Standards Working Group (2004) A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA). [Online]

Available:

[http://it.ojp.gov/documents/20041209\\_SOA\\_Report.pdf](http://it.ojp.gov/documents/20041209_SOA_Report.pdf)

U.S. Department of Justice Information Technology Initiatives (2008), Global Justice Reference Architecture [Online]

Available: [http://it.ojp.gov/topic.jsp?topic\\_id=242](http://it.ojp.gov/topic.jsp?topic_id=242)

NIEM, Building Information Systems (2008) [Online]

Available: <http://www.niem.gov>

NIEM Program Management Office (2007) Introduction to the National Information Exchange Model (NIEM). [Online]

Available: [http://www.niem.gov/files/NIEM\\_Introduction.pdf](http://www.niem.gov/files/NIEM_Introduction.pdf)

U.S. Department of Justice Information Technology Initiatives (2008), Global Federated Identity and Privilege Management (GFIPM) [Online]

Available: [http://www.it.ojp.gov/topic.jsp?topic\\_id=248](http://www.it.ojp.gov/topic.jsp?topic_id=248)

U.S. Department of Justice Information Technology Initiatives (2003), National Criminal Intelligence Sharing Plan [Online]

Available: [http://www.iir.com/global/products/NCISP\\_Plan.pdf](http://www.iir.com/global/products/NCISP_Plan.pdf)



# Whitepaper

[Archana Janakiram](#)

Enterprise Solutions Group  
Analysts International Corporation,  
ajanakiram@analysts.com

[Rob Kribs](#)

Enterprise Solutions Group  
Analysts International Corporation,  
rkribs@analysts.com

[Prem Neelakanta](#)

Enterprise Solutions Group  
Analysts International Corporation,  
pneelakanta@analysts.com

[Iveta Topalova](#)

Enterprise Solutions Group  
Analysts International Corporation,  
itopalova@analysts.com