Introduction to the
National Information Exchange Model
(NIEM)

NIEM Program Management Office

February 12, 2007
Document Version 0.3

NIEM
BRIDGING INFORMATION SYSTEMS

Table of Contents

Figures

Tables

Motivation for NIEM

The National Information Exchange Model (NIEM) is designed to develop, disseminate, and support enterprise-wide information sharing standards and processes across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise at all levels and across all branches of government.

A variety of emergency situations in recent years have demonstrated in increasingly vivid detail the tragic consequences that often result from the inability of jurisdictions and agencies to effectively share information. Terrorist attacks, natural disasters, and large-scale and organized criminal incidents too often serve as case studies that reveal weaknesses in our nation's information sharing capabilities. Moreover, enterprise-wide information sharing is also required to support the critical day-to-day operations of public safety officials at all levels and across all branches of government.

Citizens and decision makers alike largely believe that organizations today can instantly share critical information at key decision points. Contributing to this perception is the portrayal of extraordinary information sharing capabilities in television programs, movies, and other media. Surely, the public believes, first responders can share information and effectively communicate in emergency situations, when seconds count and lives are at stake.

It is an unfortunate reality that today enterprise-wide information sharing is *not* universally possible. Even though agencies across the nation perform similar operational functions and capture and use common information (e.g., data regarding people, places, and events), their internal business processes often vary from jurisdiction to jurisdiction and agencies use different information systems and technologies. What is lacking is a national mechanism to identify

> The vision for NIEM is to be the standard of choice for intergovernmental information exchange, thereby:
>
> - Enhancing the quality of governmental decision making by enabling accurate, timely, complete, and relevant information to decision makers across the broad spectrum of NIEM COIs.
> - Achieving greater efficiency, effectiveness, and return on investment (ROI) in operations by accelerating information exchange design and development.
> - Reducing risk in development efforts for practitioners and industry by having common exchange standards, tools, processes, and methodologies.
> - Improving public safety and homeland security by breaking down stovepipes enabling real-time, secure, enterprise-wide information sharing.

and facilitate broad information exchange with other agencies and jurisdictions. As a consequence, agencies are often unable to effectively share information in a timely, secure manner, and too often there are fundamental differences in the nature and understanding of information between agencies.

Courts, for example, have widely adopted sophisticated case-management systems that meet their day-to-day internal operational needs, but they often do not routinely share information electronically with other agencies throughout the justice enterprise. Similarly, law enforcement has adopted computer-aided dispatch solutions, mobile field-reporting technologies, and records-management and crime-analysis systems that meet their internal operational needs. Few communities throughout the nation, however, have successfully established integrated justice information sharing solutions that enable real-time, enterprise-wide sharing of critical data at key decision points. The result is a series of information system silos that perhaps meet the operational needs and reflect the business practices of individual organizations but are not positioned to effectively share critical data with others in support of day-to-day operations and emergency situations.

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. The result is more efficient and expansive information sharing 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 complete information, and tangible improvements in public safety and homeland security.

This *Introduction to NIEM* is designed to a) provide a general description of how NIEM functions, b) describe the need for and value of NIEM as an enabler of enterprise-wide information sharing, c) provide an overview of key NIEM concepts, and d) identify near-term goals of the NIEM program.

The Role of NIEM in Information Sharing

To identify and facilitate information sharing between agencies, the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) launched NIEM through a partnership agreement between their Chief Information Officers (CIO) on February 28, 2005. It is anticipated that this partnership will expand to other agencies of government based on their needs and the demonstrated success of the NIEM model and approach. NIEM leverages the data exchange standards efforts successfully implemented by DOJ's Global Justice Information Sharing Initiative (Global) and extends the Global Justice XML Data Model (Global JXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise.

> NIEM represents a partnership, initially between the U.S. Department of Justice and the U.S. Department of Homeland Security, and soon with other critical agencies.
>
> The current domains in NIEM include justice, intelligence, immigration, emergency management, international trade, and infrastructure protection.

NIEM complies with the Homeland Security Presidential Directive (HSPD-5), which assigns the Secretary of DHS the role of principal federal official for domestic incident management. The Homeland Security Act of 2002 charges the Secretary with the responsibility for coordinating federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Building on this foundation is a series of executive orders which direct agencies to improve the exchange of terrorism information and protect their ability to acquire information.

Rather than nationwide integration of all local, state, tribal, and federal databases, NIEM focuses on cross-domain information exchanges between key domains and communities of interest (COIs), across all levels of government—whether between individual local law enforcement agencies, law enforcement and emergency-service agencies, and other domains, or between local, state, tribal, regional, and federal agencies.

NIEM complies with Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Based on this act, the President established the Information Sharing Environment (ISE) to facilitate the sharing of terrorism information. The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use,

management, and sharing of terrorism information within the ISE, consistent with the protection of intelligence, law enforcement, military sources, methods, and activities. NIEM is identified by the ISE as a standard that provides a set of reusable common information standards.

NIEM does not attempt to normalize all information components across all agencies and organizations, only those that cross organizational boundaries and only that subset of data needed for inter- and intra-agency information exchange. NIEM is predicated on identifying operational information exchanges among participating domains by examining current practice (i.e., documenting business requirements for information exchange between agencies and domains) and by modeling new and innovative information exchange opportunities to achieve greater efficiency, effectiveness, return on investment (ROI), and new operational capabilities.

In an emergency situation, such as a building collapse, local first responders, fire departments, emergency medical services, disaster management teams, law enforcement, health officials, and other city, county, state, and perhaps federal agencies need to share critical information in real time and in a secure setting. Recognizing that the information exchange needs of agencies involved in these situations are comparable in thousands of jurisdictions across the nation (and perhaps even beyond our national borders), NIEM can facilitate the uniform and rapid development and deployment information sharing standards to expedite these critical exchanges.

> NIEM is a framework to:
> - Bring stakeholders together to identify information sharing requirements in day-to-day operational and emergency situations.
> - Develop standards, a common vocabulary, and an online repository of information exchange package documents (IEPDs) to support information sharing.
> - Provide technical tools to support development, discovery, dissemination, and reuse of IEPDs.
> - Provide training, technical assistance, and implementation support services for enterprise-wide information exchange.

NIEM Key Concepts

The following key concepts are essential to understanding the purpose, architecture, processes, and other capabilities of NIEM, as well as to establish a common knowledge base with which to develop the ability to use NIEM effectively.

Data Components

The fundamental building block of NIEM is the *data component*. Data components are the basic business data elements that represent real-world objects and concepts. Information exchanged between agencies can be broken down into individual components—for example, information about people, places, material things, and events. Components that are frequently and uniformly used in practice are specified in NIEM and can then be reused by practitioners for information exchanges, regardless of the nature of their business or the operational context of their exchanges, provided they are semantically consistent.

Some sources of data components include data models, databases, data dictionaries, schemas, and exchanges. In NIEM, these objects and constructs are represented using XML Schema for the purpose of consistent definition and transmission of information exchange packages (IEPs). The model, however, is independent of any particular technology and in the future could be depicted in any number of representations (e.g., Resource Definition Framework (RDF) or Web Ontology Language (OWL)), which would produce semantically consistent interoperable information sharing. It is anticipated that future versions may migrate to new and evolving forms.

NIEM components are not merely a set of stand-alone components to build messages; together they form a cohesive data model that attempts to provide consistent semantics and structure. To effectively exchange information, there must be a common semantic understanding of data among participating agencies, and the data must be formatted in a semantically consistent manner. Two agencies, for example, may each gather information about persons charged with committing a crime. If the agencies share information regarding these persons, there must be a common understanding of the terminology each agency uses and common attributes describing the person. One agency may refer to a person as the "arrestee," whereas another refers to the person as the "defendant," but in either case they are referring to a human being with minimal attributes that can be mutually agreed upon between the agencies (e.g., a person with a given name, age, sex, or race). Agencies do not necessarily need to entirely retool their information systems or adopt standards and coding schemes that impose an artificial uniformity in data collection that fails to meet their operational business needs, but there must be common understanding and semantic consistency in the structure of the data that crosses agency lines if it is to be successfully shared.

NIEM Core

Data components within an information exchange that are universally shared and understood among all (or almost all) domains are identified as *universal components* (e.g., person, address, and organization). To become a universal component, consensus by all domains is needed on the semantics and structure of the component. The set of NIEM universal components is stable (once established) and relatively small.

A data component, such as a person, represents a composite of attributes which describe something of interest—in this case, a person. The component may include such attributes as the person's name, date of birth, sex, race, ethnicity, height, weight, eye color, hair color, or body type. The *person component* is used in nearly all relevant agency or domain information systems that are presently affiliated or likely to be affiliated with NIEM in the future; e.g., police information systems (where the person may be a suspect, an arrestee, a witness, or a victim), court case-management systems (where the person may be a defendant, a plaintiff, a witness, an attorney, or a juror), health-care systems (where the person may be a patient, doctor, or health-care worker), and transportation systems (where the person may be a passenger, a flight attendant, or a transportation worker), and it carries the same meaning across all the COIs. Thus it is classified as *universal*.

Once the person component has been defined and validated in operational use, it can be stored in NIEM and made readily available for discovery and reuse by other interested COIs. Its semantic definition will persist beyond any technology in use today, bringing all the COIs to true interoperability without artificial translators or middleware. As a consequence, COIs need not spend the time and effort ordinarily required to construct a component from scratch, and it facilitates greater information sharing, making connections more expansive and expedient.

As shown in *Figure 1: Component Reuse*, each NIEM domain can extend *universal* for its own use, and *person* may have different attributes within these other domains. In this example, the person component used in *universal*, identified as U:Person, is extended by addition of other components in the justice domain forming J:Person, and J:Person is similarly extended to IM:Person for use in Immigration exchanges.
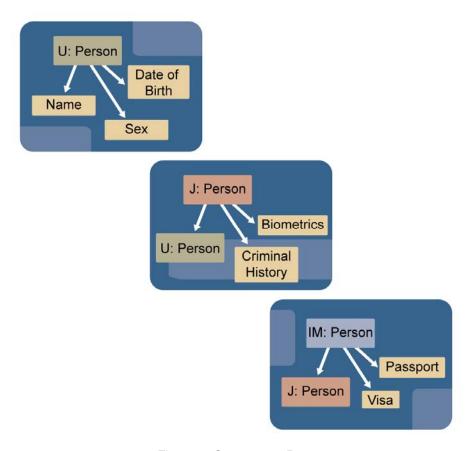
Figure 1: Component Reuse

A robust harmonization process, which is explained in more detail in the *NIEM ConOps* and the *NIEM User Guide*, will operate to ensure that a) ***universal*** and ***common components*** are effectively defined, b) components are governed by a process that provides effective voice and involvement among all domains and COIs with a stake in the components, and c) NIEM remains a consistent and coherent data model.

Domains

For purposes of NIEM, a domain refers to a business enterprise broadly reflecting the agencies, units of government, operational functions, services, and information systems which are organized or affiliated to meet common objectives. NIEM domains are organized to facilitate governance, and each has some measure of persistency. Each domain traditionally includes a cohesive group of data stewards who are subject-matter experts (SMEs), have some level of authority within the domains they represent, and participate in the processes related to harmonizing conflicts and resolving data-component ambiguities.

Domains are expected to:

- ❖ Provide content to NIEM;
- ❖ Provide domain subject-matter expertise to support content development;
- ❖ Have existing COIs or the ability to enroll or formulate COIs;
- ❖ Possess the ability to perform outreach to relevant COIs;
- ❖ Support their own governance;
- ❖ Participate in NIEM governance as appropriate;
- ❖ Maintain strategic alignment within the scope of NIEM;
- ❖ Agree to the principles and practices of NIEM (including conformance to NIEM Naming and Design Rules (NDR);
- ❖ Maintain alignment with the NIEM taxonomy; and
- ❖ Authoritatively support internal and external harmonization.

One such domain currently engaged in NIEM is Justice. The Justice domain includes agencies whose functions relate to the reporting and investigation of crime, the apprehension of suspected offenders, the prosecution and adjudication of those charged with criminal offenses, the correctional confinement and supervision of those convicted, and other appropriate duties and functions. Other NIEM domains currently addressed in NIEM include Intelligence, Immigration, Emergency Management, International Trade, and Infrastructure Protection.[1] *Figure 2: NIEM Core and Domains* shows the relationship between NIEM core and NIEM domains.

---

[1] The Justice domain is largely represented in NIEM by the Global Justice Information Sharing Initiative: http://www.it.ojp.gov. The Emergency Management domain is largely represented by the OASIS Emergency Management Technical Committee: http://xml.coverpages.org/emergencyManagement.html#oasis. The Intelligence domain is largely represented by the Intelligence Community Metadata Working Group: https://www.icmwg.org/. The Critical Infrastructure Protection Initiative is largely represented by the Open GIS Consortium: http://www.opengeospatial.org/.
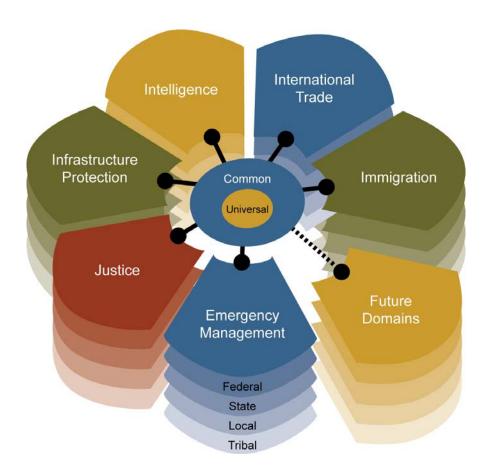
Figure 2: NIEM Core and Domains

The ability to exchange information using NIEM, however, is not limited to NIEM domains. There are NIEM mechanisms for accessing and including information residing in domains that are external to NIEM within NIEM-conforming IEPDs. These external domains represent data standardization initiatives outside the scope of NIEM and do not fall under the *NIEM NDR* or governance processes. Nevertheless, there are multiple ways for an external domain to interact with NIEM, including validating the external domain against the NIEM reference schema. More information on how external domains and their COIs can participate in NIEM is available in the *NIEM Concept of Operations (NIEM ConOps)*.

Communities of Interest

Communities of interest (COIs) are collaborative groups of users who exchange information in pursuit of shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they

exchange.[2] Generally, COIs are formally constituted through an organizational charter, a memorandum of understanding (MOU), articles of incorporation, or the Federal Advisory Committee Act (FACA).[3]

COIs reuse data components and artifacts found in NIEM to document their information exchanges. One or more COIs can coordinate to develop new domain content as they identify gaps in the data components needed for documenting information exchanges. COIs typically meet, either personally or virtually, to articulate and define their business requirements and to plan, map, and model their inter- and intradomain information sharing requirements.

Information Exchange Package Documentation

The information that is commonly or universally exchanged between participating domains can be organized into *information exchange packages* (IEPs) in the form of XML Schemas. An example of this collection of information is data associated with an arrest. The data to be exchanged includes not only descriptive and personal identification data regarding the individual arrested (i.e., the person component described above) but also information about the person's alleged offense, the location of the offense, the arresting officer, etc. The IEP represents a set of data that is actually transmitted between agencies for a specific business purpose (e.g., initiating a charging document by the local prosecutor). It includes the actual XML instance that delivers the payload or information. Additional information regarding this specific exchange can be further documented in the form of an information exchange package documentation (IEPD), which also contains data describing the structure, content, and other artifacts of the information exchange. An IEPD supports a specific set of business requirements in an operational setting.

NIEM provides a library of reusable objects for building information exchange package *templates* in the form of XML Schemas defining the exchange message content (i.e., content payload*).* The payload is enclosed in a "message," which provides routing information and associated security controls needed to deliver the content. Exchange packages include both document exchanges (e.g., an immigration form, alert, or incident report) and database queries and responses

---

[2] DoD Chief Information Officer Memorandum "DoD Net-Centric Data Strategy," May 9, 2003, http://www.dod.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf

[3] More information regarding the Federal Advisory Committee Act can be found at http://www.archives.gov/federal-register/laws/fed-advisory-committee/. Organizational charters for other COIs can be found at http://xml.coverpages.org/emergencyManagement.html.

(e.g., a vehicle license-plate search run against a stolen-vehicle database). NIEM reusable objects can be used for both structured and unstructured query/responses.

Figure 3: Relating IEPDs to IEPs shows the relationship between IEPs and the NIEM model.
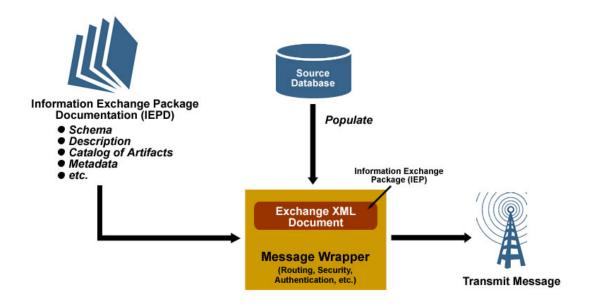

Figure 3: Relating IEPDs to IEPs

NIEM standardizes the artifacts necessary for interagency information exchange into an IEPD. NIEM is designed to make IEPDs available to users in tools that enable efficient and intuitive search and discovery. In this way, users will be able to discover and reuse existing IEPDs that meet their operational requirements. In addition, users may also extract and reuse specific content that has been used in published IEPDs to build their own IEPDs. NIEM creates and disseminates tools to support rapid IEPD development and deployment and provides managed processes for the creation, support, dissemination, and implementation of information exchanges. In order to support these exchanges, NIEM provides:

❖ A central location that allows for the registration, discovery, and reuse of IEPDs that have been certified by authoritative sources;

❖ Means to ensure that IEPDs are developed using established, conventional methodologies that result in machine-readable, easy-to-understand artifacts.

The NIEM IEPD life cycle (see *Figure 4: IEPD Life Cycle*) provides an illustration of how IEPDs are ideally built and published. This life cycle is not intended to be prescriptive; i.e., IEPD developers may enter the life cycle at any particular step and may adjust the scope of the life cycle to support the level of effort needed for their IEPD development. Neither are timeframes for completion of each step of the life cycle predefined, as these will be determined by the business needs of the user. The *NEIM ConOps* provides more detail on the IEPD life cycle.

IEPDs include:
- XML Schemas that use or correctly extend NIEM components and define a class of XML exchange instances, subset schema want lists, and style sheets.
- Documentation on implementing the IEP with the schemas as well as other documentation such as business requirements, memoranda of understanding, domain models, use-case models, and business rules.
- IEPD artifacts, including the manifest (list of artifacts in the IEPD) and the metadata registered with the IEPD that is used for indexing, search, discovery, maintenance, registration, etc.
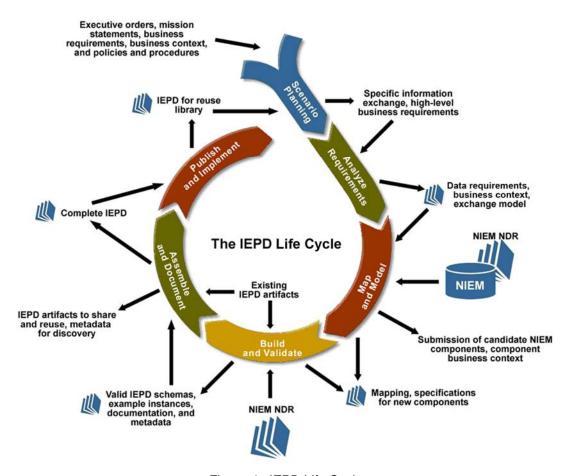
Figure 4: IEPD Life Cycle

Scenario Planning

Not all the information an organization collects, of course, needs to be shared with other organizations or domains. Identifying precisely what information is exchanged between organizations can best be determined by modeling relevant business practices through scenario-based planning and information exchange mapping.

Organizations define information exchanges to support the sharing of information in real-life scenarios. Scenarios describe the business context of events, incidents, or circumstances in which information must be exchanged between agencies and/or domains. The scenario may be a terrorist attack on a city, a natural disaster, a major criminal incident requiring response by multiple agencies or jurisdictions, or simply the day-to-day operations of justice, public safety, and homeland security agencies at all levels of government.

Scenario planning can be completed from a bottoms-up approach, which depicts either current information exchanges among involved parties or potential future environments that envision broader and more expansive information sharing, as well as changes in business practices. In this form of scenario planning, users or a COI may identify a specific information exchange for IEPD development based on critical business functions or operational priorities.

Scenarios can also be constructed from a top-down approach, through the use of business taxonomies. Business taxonomies document the business operations of an organization using a common framework, such as the FEA BRM. The FEA BRM taxonomy categorizes an organization's operations by lines of business (LoBs) and subfunctions. Agencies have the flexibility to extend the BRM to support their business requirements. It is at the process level where exchange points describing specific business events will be identified and correlated to IEPDs, which can be developed to affect the exchange of business information. In either situation, scenario planning can assist in identifying gaps, impediments, and other flaws in business processes and data exchanges. More detail regarding these approaches is found in the *NIEM ConOps*.

Whichever approach a developer takes—bottoms-up or top-down—the result is the identification of specific information exchanges which are the objective of IEPD development. This preliminary step of identifying the operational context of information exchange is a critical prelude to development of effective IEPDs, in which the business and operational context of information sharing is established and articulated.

Careful elaboration of business scenarios can identify critical operational points at which information must be shared between two or more parties. The scenario below is an example demonstrating the breadth and scope of information sharing requirements in operational settings. Scenarios such as the one below identify the operational context, the business value, and the nature of the information that needs to be exchanged. Such scenarios almost invariably reveal a constellation of exchanges that are required to satisfactorily enable an effective operational response, and such exercises may well engage a rich variety of domains and COIs. The specific exchanges inherent in this scenario are indicated in **bold**.[4]

---

[4] More sample scenarios can be found in the *NIEM ConOps*.

The 911 Emergency Operations Center (EOC) of a mid-sized urban jurisdiction begins receiving telephone calls from residents regarding what is variously described as a fire, an explosion, and a partial building collapse of a 25-story building in the city center. The calls, which quickly escalate in number and urgency, are received from residents of the affected office building, local residents of other nearby buildings, and pedestrians and passing motorists using cellular telephones.

The EOC dispatches police, fire units, and emergency medical personnel. The cause of the damage and the fire, as well as the extent of the damage and scope of the emergency, takes time to establish. **First responders arriving on scene begin reporting to the EOC on the nature and scope of the damage**, which is extensive and may well result in a catastrophic collapse of the entire building and potentially extensive damage to surrounding buildings. Initial on-scene units find the aftermath of a significant explosion with several ongoing fires and many "walking wounded" wandering throughout the incident scene.

Police and fire units initiate a command post across the street from the incident location. Police units establish a critical perimeter for public safety entry only and begin initiation of a secondary perimeter using geographic information system (GIS) mapping. Emergency Medical Services (EMS) personnel set up an initial triage contiguous to the police and fire command post. **Initially injured persons are assessed, and information is forwarded to area hospitals via devices that track hospital capacities, services available, and patient transports.**

Real-time video feeds are transmitted from the scene to the command post. Personnel location technology is in use providing 2D/3D location and biotelemetry of fire and police personnel to their command staffs, as well as monitoring of immediate air quality in proximity to the explosion site. Upon completion of the first search, the scene is declared unsafe and messages are sent to all on-scene personnel to remain outside the critical perimeter until the scene is cleared by the bomb squad. The media is kept informed of progress, as appropriate.

The scenario described above demonstrates the data exchanges, communications interoperability, and closely aligned business practices that are inherent in operational information sharing. As this scenario demonstrates, immediate, secure, enterprise-wide information sharing and interoperable communications are required to facilitate tightly coordinated response across multiple agencies, domains, and jurisdictions.

Although many of the exchanges described in the scenario above are possible today, they must often be done in a serial, labor-intensive manner, utilizing specific codes pertaining to each legacy system being queried. Too often agencies and jurisdictions lack the ability to securely share critical information in real time. NIEM is designed to enable efficient and effective information sharing through the use and reuse of robust information exchange standards.

NIEM Resources and Processes

NIEM includes a set of operational processes and procedures, standards, documentation, tools, training, and technical assistance.

Capability	Description
Documentation	❖ *Introduction to NIEM* ❖ *NIEM Concept of Operations* (ConOps) ❖ *NIEM User Guide* (to be developed after the release of NIEM 1.0) ❖ *NIEM Naming and Design Rules* (NDR)
Training and Technical Assistance	❖ Training materials ❖ Briefings and executive materials ❖ Process-related documentation ❖ Help desk and knowledge base
Tools	❖ Set of tools freely available with each NIEM release ❖ Implementation of all structural and content features of the release ❖ Support activities such as scenario-based planning, information exchange mapping and modeling, and IEPD generation
Governance and Processes	❖ Structure to manage and maintain NIEM ❖ Processes and procedures behind its operations including oversight and approval bodies for the interaction of NIEM domains and external domains, development of IEPDs, and data model maturity

Table 1: NIEM Functions

NIEM represents a working and collaborative partnership among key governmental agencies, operational practitioners, technologists, systems developers, solution providers, standards bodies, and other stakeholders at all levels of government and across the broad landscape of the justice, public safety, and homeland security enterprise. Effective governance requires executive support and investment, senior policy guidance, strategic partner engagement, operational support and direction, technical development and implementation,

and broad communication and outreach activities. The initial governance structure of NIEM reflects these broad and diverse responsibilities and participants (see the NIEM *ConOps* for a more complete discussion of NIEM governance).

NIEM's operations are dependent upon its stakeholders. It functions to bring stakeholders of relevant communities together to define information exchanges and to provide them the necessary tools and support mechanisms to facilitate adoption of common standards for enterprise-wide information exchange. Governance of NIEM is designed to mature as the program evolves, to remain agile in order to respond to the emerging needs of an ever-expanding community of users, and to reflect the national scope and federal sponsorship of the NIEM program, while actively engaging agencies, organizations, and practitioners at all levels and branches of government.

Private sector solution providers also continue to be equal partners in NIEM through various representative organizations, such as the IJIS Institute, the Organization for the Advancement of Structured Information Standards (OASIS), and the Emergency Interoperability Consortium (EIC), among others. The active involvement of business and technical representatives will ensure operational integrity and a comprehensive perspective in the standards being developed. Industry plays a critical role in developing, validating, and implementing NIEM-supported standards, as well as recommending new NIEM content and support and development processes and tools.

Understanding the Value of NIEM

Providing immediate access to timely, complete, and relevant information, and sharing critical data at key decision points throughout the whole of the justice and public safety enterprise are key objectives of the NIEM program. Fundamentally, NIEM is not just about technology or making systems perform better. Rather, it is about making major improvements in the way information is shared throughout the nation. NIEM's primary value propositions include:

❖ Enhancing the quality of governmental decision making by enabling accurate, timely, complete, and relevant information to decision makers across the broad spectrum of NIEM COIs;

❖ Achieving greater efficiency, effectiveness, and return on investment (ROI) in operations by accelerating information exchange design and development;

❖ Reducing risk in development efforts for practitioners and industry by having common exchange standards, tools, processes, and methodologies; and

❖ Improving public safety and homeland security by breaking down stovepipes enabling real-time, secure, enterprise-wide information sharing.

NIEM aims to achieve these value propositions through several attributes:

NIEM Desired Attributes	
Accessibility	❖ NIEM, in all of its attributes, is understandable by its stakeholders on their terms and based on a reasonable investment of time and energy. ❖ NIEM reflects conceptual integrity, such that mastering a handful of documented principles provides a framework for understanding. ❖ The NIEM community is encouraged to provide input, which is incorporated into NIEM releases, tools, documentation, etc.

Semantic Integrity	❖ NIEM products are viewed and vetted by the stakeholder community, are frequently iterated, and reflect a focus on measurable improvement of quality. Domain entities:
	   – are reflected in the model in a consistent manner;
	   – use the model and governance constructs in a consistent manner; and
	   – are documented in a complete and actionable manner.
	 ❖ Quality is measured through increasing levels of reuse and completeness, and decreasing levels of inconsistency or changes that are not attributable to new business conditions, stakeholders, or model capabilities.

NIEM Desired Attributes (continued)	
Low Total Cost of Ownership	❖ Consistent use of NIEM, in conjunction with external architectural best practices, results in measurable cost savings, both up-front and ongoing, for stakeholders. Savings come from: – analysis and development methodology; – building fewer and more generalized exchanges; – reuse of exchanges and data components; – leverage of NIEM outreach, training, and help desk; and – leverage of existing NIEM governance structures.
Scalability	❖ NIEM stakeholders can conduct cross-domain information exchanges. – NIEM COIs need to be able to support exchanges between participating and external domains. – External domains that see some of their stakeholders participating in NIEM COIs should be able to assess the value in joining NIEM. ❖ The value proposition for NIEM stakeholders gets stronger with growth in the stakeholder community and, by extension, growth in the number of participating domains.

Table 2: NIEM Desired Attributes

Figure 5: Role of NIEM in Information Sharing illustrates how NIEM simplifies information sharing to improve accuracy, efficiency, and speed.
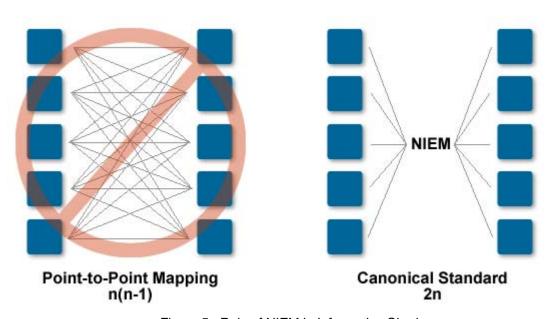

Point-to-Point Mapping
n(n-1)

Canonical Standard
2n

Figure 5: Role of NIEM in Information Sharing

Early anecdotal evidence illustrates the tangible business value of using common information exchange standards: The Missouri Office of State Courts Administrator (OSCA) reports that using the Global JXDM has reduced development time by 50 percent, reducing conversion time from 18 to 24 months to 6 to 9 months, with potential savings of $1.6 million over two years.

A comprehensive program of performance measurement is being created to assess the ongoing business value and operations of NIEM across each of the dimensions associated with the NIEM value propositions.

NIEM Near-Term Goals

NIEM development is an iterative process. The processes, standards, documentation, and tools that are part of NIEM will continue to be reviewed and updated as NIEM grows in scope and scale. Moving forward, NIEM efforts will concentrate on:

Goal	Description
Core Capability Development and Maintenance	❖ Delivering NIEM releases ❖ Fully implementing NIEM governance ❖ Representing the critical mass of justice, homeland security, and intelligence information exchanges in their associated domains ❖ Developing a tools road map based on user requirements and delivering the tools into operation ❖ Launching outreach activities (including the Web site), conference presentations, and training
Information Exchange Standard Development	❖ Developing families of IEPDs representing core, priority business areas at the national level (examples include incident reporting, people screening, suspicious activities, cargo screening, emergency and disaster management, and case management) ❖ Working with appropriate authoritative sources to champion the development of national priority exchanges (e.g., support the Program Manager of the ISE in developing counterterrorism IEPDs)

Goal	Description
Outreach and Implementation	❖ Catalyzing NIEM adoption and usage with stakeholders ❖ Deepening partnerships with COIs ❖ Identifying additional pilots at the local, state, and tribal levels, targeting the emerging national exchange standards mentioned above ❖ Implementing the infrastructure needed for tools, training, and technical assistance, including a help desk ❖ Harmonizing data components across information domains

Table 3: NIEM Near-Term Goals

Conclusion

The *Introduction to NIEM* is the first in a series of four documents providing stakeholders the information they need to participate in NIEM. The *NIEM ConOps, User Guide,* and *Naming and Design Rules* will follow and are recommended for further review. Each of the documents builds on content put forth in the previous document to eliminate redundancy and ensure clarity.

Figure 6: NIEM Reading Road Map describes the nature and scope of each of these documents.

Introduction to NIEM

The document you are reading.

This document provides a background on NIEM, and a high-level overview of NIEM, focusing on the business needs and value propositions to the key stakeholders. It describes how NIEM aids information sharing in a real-life scenario such as a terrorist attack or natural disaster. *The Introduction to NIEM* answers the following questions:

- What is NIEM?
- What is the value of NIEM?
- Who is using NIEM?
- How does NIEM relate to information sharing today?

NIEM Concept of Operations (ConOps)

This document describes the NIEM development approach, the management and governance structure, and the operational processes and procedures related to NIEM. The *ConOps* answers the following questions:

- Do you want to participate in NIEM?
- How do you participate in NIEM?
- How would you interact with NIEM processes and procedures?
- Where can you find more information on NIEM?

NIEM User Guide

This document serves as a set of tutorials on how to use NIEM. It provides more detail on how stakeholders participate in the NIEM processes and procedures as well as more detail on the NIEM technical architecture. The *User Guide* answers the following questions:

- Where can you find more information related to specific topics?
- Who are the key points of contact?
- How can you complete specific tasks (e.g., create an information exchange package)?

NIEM Naming and Design Rules

This document governs the identification and definition of NIEM components and provides the technical principles and rules for NIEM XML conformance. Its primary audiences are the practitioners and developers who employ NIEM for information exchange and interoperability. The *NDR* answers the following questions:

- What does it mean to be NIEM conformant?
- What are the normative rules for building NIEM schemas and instances?
- How may NIEM-conformant subsets be created, extended, constrained, and used to define reusable NIEM information exchanges?

Figure 6: NIEM Reading Road Map

Appendix A: Glossary

The following list is a subset of key terms and their definitions, which are necessary to understand the core concepts discussed in this document. The complete NIEM Glossary can be found on www.NIEM.gov.

❖ Common Component: Components used in exchanges between two or more domains, but not universally shared.

❖ Community of Interest: Collectives of people composed of practitioners and technical representatives (government and private sector) who, by virtue of their organizational affiliation, day-to-day operational responsibilities, or provision of services and programs collectively, have a stake in NIEM information exchanges and who authoritatively represent their respective domains.

❖ Data Component: Basic business data items that represent real-world objects and concepts. Information that is exchanged between agencies can be broken down into individual components—for example, information about people, places, material things, and events.

❖ Data Dictionary: A set of metadata that contains definitions and representations of data elements.

❖ Data Model: A graphical and/or lexical representation of data, specifying their properties, structure, and interrelationships.

❖ Discovery: The act of locating a machine-readable description of a Web service-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. For NIEM, discovery normally refers to the search of IEPDs within a repository to identify data components that can be reused in IEPD development.

❖ Domain: Business enterprise broadly reflecting the COIs, agencies, units of government, operational functions, services, and information systems which are organized or affiliated to meet common objectives.

❖ Domain-Specific Components: A component that meets technical standards, complies with NIEM requirements, and is specific to only one domain, which is managed and harmonized by a COI.

❖ Extensible Markup Language: XML is a structured language for describing information being sent electronically from one entity to another. XML Schema defines the rules and constraints for the characteristics of the data,

such as structure, relationships, allowable values, and data types. NIEM does not use document type definition (DTD); it only uses XML Schemas.

❖ Framework: A specific implementation of a component architecture.

❖ Governance: The system and manner of providing authority and control.

❖ Information: Contextual meaning associated with, or derived from, data.

❖ Information Exchange Package: A set of data elements used to support the sharing of data within a particular business context. An actual set of data that is requested or produced from one unit of work to another.

❖ Information Exchange Package Documentation: A collection of artifacts that define and describe the structure and content of an IEP.

❖ Message: The basic unit of communication between a requester and a provider; it should encompass IEPDs relevant to the message exchange.

❖ *NIEM Naming and Design Rules*: The *NIEM NDR* specifies an information sharing framework. These rules and principles are intended to establish and, more importantly, enforce a degree of standardization at the national level.

❖ Repository: An information system used to store and access architectural information, relationships among the information elements, and work products. For NIEM, the repository includes the data dictionary, data model, IEPDs, and data components that comprise them.

❖ Stakeholder: A person or organization that has a legitimate interest in a project or entity; anyone with an interest (or stake) in what the entity does.

❖ Universal Component: A component that meets technical standards, complies with NIEM requirements, is defined in universally acceptable terms across all participating domains, and is reusable.

Appendix B: Acronyms

- ❖ The following is a list of acronyms found in this document.
- ❖ CIO: Chief Information Officer
- ❖ COI: Community of Interest
- ❖ ConOps: Concept of Operations
- ❖ DHS: U. S. Department of Homeland Security
- ❖ DOJ: U. S. Department of Justice
- ❖ EIC: Emergency Interoperability Consortium
- ❖ ESC: Executive Steering Council
- ❖ FACA: Federal Advisory Committee Act
- ❖ Global: Global Justice Information Sharing Initiative
- ❖ Global JXDM: Global Justice XML Data Model
- ❖ HSPD: Homeland Security Presidential Directive
- ❖ IAFIS: Integrated Automated Fingerprint Identification System
- ❖ IEP: Information Exchange Package
- ❖ IEPD: Information Exchange Package Documentation
- ❖ IRTPA: Intelligence Reform and Terrorism Prevention Act
- ❖ ISE: Information Sharing Environment
- ❖ MOU: Memorandum of Understanding
- ❖ NDR: Naming and Design Rules
- ❖ NIEM: National Information Exchange Model
- ❖ OASIS: Organization for the Advancement of Structured Information Standards
- ❖ PMO: Program Management Office
- ❖ ROI: Return on Investment