



National Capital Region Interoperability Program

NCR Data Exchange Hub Technology Guidelines

June 2006



NCR Interoperability Program

NCR DEH Technology Guidelines

Table of Contents

1	Overview	1
2	NCR DEH role in incident management	2
3	Purpose of the Guidelines	4
4	Recommended guidelines	4
4.1	Data/information guidelines	6
4.2	Integration/middleware guidelines	8
4.3	Security/privacy guidelines	11
4.3.1	Note on mobile device security	16
5	Glossary	17
Appendix A: References		21

List of Tables

<i>Table 1. NCR Data Exchange Hub: Types of Interoperability</i>	<i>3</i>
<i>Table 2. NCR Data Exchange Hub: Architecture Guidelines for Information Domain</i>	<i>7</i>
<i>Table 3. NCR Data Exchange Hub: Architecture Guidelines for Interoperability Middleware Domain</i> ..	<i>9</i>
<i>Table 4. NCR Data Exchange Hub: Architecture Guidelines for Security/Privacy Domain</i>	<i>12</i>
<i>Table 5. NCR Data Exchange Hub: Security – Related Guidelines to Assure Operational Reliability, Availability, And Maintainability</i>	<i>15</i>



NCR Interoperability Program

NCR DEH Technology Guidelines

1 Overview

The National Capital Region Data Exchange Hub (NCR DEH) Technology Guidelines, hereafter called Guidelines, are issued to support the establishment and maintenance of a regional approach for sharing data and processes among jurisdictions and Emergency Support Functions (ESFs). These Guidelines are also intended to maintain and respect jurisdictional business, privacy and security needs. Emphasizing interoperability, modularity, and reuse, these Guidelines are the first step in establishing the standards and best practices for creating, maintaining, and sharing both structured and unstructured data and emergency preparedness and response functions across jurisdiction and ESF boundaries.

This document provides an initial set of Guidelines based on current government and industry open standards and practices, both nationally and within the NCR. It includes the results of work between the NCR Interoperability Program (NCRIP) and industry groups, government data exchange initiatives, existing data sharing programs in the NCR, and state and local agencies. This work has refined and evolved these guidelines into a document that provides meaningful standards, best practices, technology profiles, and a data exchange reference model to guide the continuation of data sharing programs in the NCR.

These Guidelines reflect the principles of a Service Oriented Architecture (SOA), which is a modern approach for integration and sharing of data. SOA enables different jurisdictions and agencies to integrate data from their systems while retaining complete control of their systems and the internal architecture. There are many abstract guidelines, reference models, descriptions of functional layers and sets of specific standards or software that fulfill SOA requirements. However, within the realm of emergency and disaster preparedness and response, there are currently a shortage of clear, working examples based on real needs and requirements. These Guidelines are offered as a reference – a set of standards, organized in such a way that they can be fulfilled by a variety of technologies and products.

The current version of Guidelines focuses on the dimensions most critical to interoperability in a SOA - data/information, integration/middleware, and security/privacy. Other dimensions will be added as the data exchange architecture and reference model evolve.

An earlier version of this document was distributed to NCR Urban Area Security Initiative (UASI) program managers for their use and implementation. In order to maintain a consistent, regional approach to data sharing, it is encouraged that ESFs follow these Guidelines as they propose data sharing and/or interoperability solutions, both for new programs and for currently approved programs. Subsequent revisions of this document will be similarly incorporated into each year's sub-grant application instructions, beginning with FY2007 DHS grant applications. Applicants for sub-grants will be required to demonstrate how their program complies with these guidelines as part of their grant application.



2 NCR DEH role in incident management

Each jurisdiction within the NCR is responsible for its local boundaries and missions. These missions often cross boundaries and normal agency functions when a regional incident occurs. Information sharing in these cases often comes via costly, small “throw away” solutions designed to meet the immediate mission and goals of the situation, and often misses the mark for the greater population. In acknowledgement of this, in March 2004, the Department of Homeland Security (DHS) established the National Incident Management System (NIMS) Guidelines to help facilitate information exchange at all jurisdictional levels and across functional disciplines.

NIMS provides a framework for locales, tribes, territories, the States, and the Federal Government to work together to respond to national incidents. An information technology (IT) SOA holds the same promise for the flow of information between disparate IT systems as NIMS does for facilitating procedural and response action coordination between First Responders from different agencies or jurisdictions. Using NIMS, personnel from different jurisdictions or occupation skills can communicate about incident management in the same, mutually understood structure using similar terminology. Using SOA, IT systems that store their data in different systems, with different software and data structures, can communicate via a mutually understood IT structure. This enables the information systems already deployed in the region to maintain their primary role, while at the same time contributing to the information needs of other emergency response organizations within the region.

A SOA-based NCR DEH will ensure device independent accessibility to information and services. This access will provide subscribers meaningful use of diverse data in real world tactical scenarios. While access to the data can be provided through use of common standards and protocols, extraction of data from one entity in which it is produced, for use by another entity within a different context, can present a challenge. To address this challenge, it is imperative that we remember that *SOA is not a product or technology that can be purchased*. Instead, it is a composition of business processes and data designed to enable entities to, in the case of the NCR DEH, share information securely and efficiently. Implementing a SOA for the NCR DEH requires:

- the alignment of processes across entities to preserve the meaning of data,
- the definition of a bundle of governance-related capabilities necessary to achieve interoperability. Gartner refers to this bundle as a Web Services Framework¹.

Although a concerted effort in many aspects of public organizations will be required to achieve smooth interoperability across jurisdictions and ESFs, a Web Services Framework and process alignment require a group of commonly used standards and protocols. The NCR DEH approach fosters a collaborative communications environment through which members can collect and disseminate information amongst and between themselves, as well as with Federal and state agencies involved in securing the NCR. The project is designed to enhance the ability of emergency responders to support their Chief Administrative Officers (CAOs) and other key stakeholders within their jurisdictions by providing secure voice, video, and data communication and collaboration tools to facilitate regional situational awareness, rapid collaborative discussion,

¹ L. Frank Kenney, Daryl C. Plummer and Whit Andrews, *Strengthen Your Web Services Framework With the Right Combination of Technologies and Products*, March 9, 2005, Gartner, Inc. Publication Number G00126007.



NCR Interoperability Program

NCR DEH Technology Guidelines

and coordination and tracking of authorized actions while preventing, preparing for, responding to, and/or recovering from emergencies or disasters.

The ultimate goal of the NCR DEH is to provide a robust and secure architecture that supports interoperability. Interoperability may occur at various levels within an open system. The table below describes the various types of interoperability:

Table 1. NCR Data Exchange Hub: Types of Interoperability

Concepts of Interoperability	
Application Level Interoperability	Agencies or organizations use the same application to perform the same business functions. Shared applications are useful if the application is built specifically with that purpose in mind. <i>Example: WebEOC has a "checkbox" to mark "significant events" that are then shared regionally.</i>
Data Level Interoperability	Agencies or organizations use standards-based technologies to share specific data elements in specific ways. CAD-to-CAD data level interoperability would include the ability to "push" event and resource data from one CAD system to another in order to enable organizations to "pull" an event into their CAD systems.
Portal Level Interoperability	Portals enable communities of interest to share data that is of relevance to each through a common interface or portal. Portal level interoperability provides the option to offer several services via a single portal and to address multiple communities of interest that may have an overarching goal such as homeland security. Portals bring streams of data to particular communities of interest and enable the use of filtering, chat functions and other tools and capabilities. Portal level interoperability relies on standards-based data level interoperability.

Application Level Interoperability is facilitated within each ESF with jurisdictions deploying similar applications across the region. The deployment of the WebEOC application for all Emergency Operations Centers (EOC's) in the region is an example of Application Level Interoperability. Standardizing nomenclature (data elements) for all emergency service resources across the region, mapping those data elements to a standardized XML schema, and then implementing that schema throughout the region in order to integrate data from the different jurisdictions is an example of how the NCR DEH will support and promote *Data Level Interoperability* to the benefit of all participants. *Portal Level Interoperability* will be supported by the development of an NCR DEH IT Services Portal to provide regional access to draft policies and procedures, ESF IT system and project inventories, and life cycle development artifacts.



NCR Interoperability Program

NCR DEH Technology Guidelines

3 Purpose of the Guidelines

The purpose of this document is to identify and disseminate the Guidelines to all regional ESF based data sharing projects so that their implementation may be compatible with the NCR agreed upon architecture standards and principles. These Guidelines and the underlying principles are intended to enable projects to interface with other projects and prevent inappropriate “silo” solutions. This document addresses the standards that are useful and effective when applied to the process of evaluating, developing, modifying, protecting, and sharing the state/local/Federal information assets of the NCR in all its forms and throughout its life cycle.

This document will serve to support applications used by the NCR Emergency Managers, CAO’s, and senior elected officials of their jurisdictions by providing secure voice, video, and collaboration tools to facilitate regional situational awareness, rapid collaborative discussion of options for action, and the coordination and tracking of authorized actions while preventing, preparing for, responding to and/or recovering from emergencies or disasters.

This document is predicated on the assumption that, to achieve any level of interoperability, all new NCR ESF technical architectures should be based on an open systems approach. The jurisdictions in the NCR are committed to leveraging open standards, both in a regional solution and in their internal governance. The rationale for this assumption follows:

- Regional information architectures involve integration of information systems and data across diverse, federated agencies and jurisdictions. This implies that a solution will utilize commonly available, vendor-neutral, open standards but not prescribe a specific implementation or product for an agency or jurisdiction.

The following implications of this assumption are as follows:

- Resources, information, and software components can be shared. Lifecycle costs should be minimized.
- The architecture will accommodate the large inventory of legacy systems built on proprietary components.
- To be effective, organizations within the NCR must collectively encourage vendors to provide products based on open systems standards.
- Continued coordination will be required to resolve and interpret the open standards as real-world NCR systems are implemented.

4 Recommended guidelines

Architectural dimensions are often referred to as “domains”. SOA-based standards are identified to guide the definition of service interfaces and messages in each domain. This document is focused on identifying and grouping standards for the domains most critical to NCR interoperability: information/data, integration/middleware, and security/privacy. This initial list was derived from information contained in the [Federal Enterprise Architecture \(FEA\) Technical Reference Model \(TRM\)](http://www.whitehouse.gov/omb/egov/a-6-trm.html)² as outlined below:

² White House, *Federal Enterprise Architecture Technical Reference Model*. Retrieved April 24, 2006 from <http://www.whitehouse.gov/omb/egov/a-6-trm.html>.



NCR Interoperability Program

NCR DEH Technology Guidelines

- The information domain describes the logical structure of data and processes and the methodology used to correlate data and processes across multiple data stores and jurisdictional entities.
- The integration domain describes a service oriented set of interfaces to make it easier to communicate among users and legacy and server environments in a distributed infrastructure environment independent of network and platform technologies.
- The security domain describes the features necessary to ensure the privacy and accessibility of information.

The [Federal Enterprise Architecture \(FEA\)](#), is a business-based framework for government-wide improvement that is entirely business-driven. Its foundation is the Business Reference Model, which describes the government's lines of business and services. This business-based foundation provides a common framework for improvement in a variety of key areas.

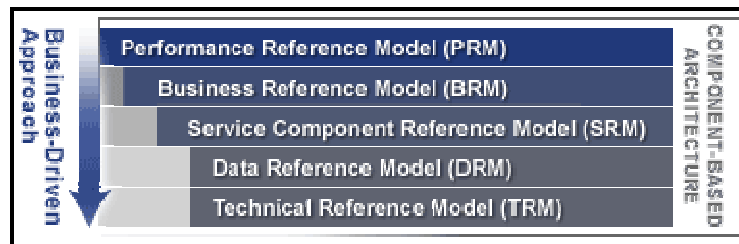


Figure 1. NCR Data Exchange Hub: FEA Consolidated Reference Model (CRM)³

The FEA CRM provided the NCR DEH Project Team with great insights into establishing a data reference model, business reference model and service reference model for the DEH. And the TRM was the foundation for the technical assessment. For a detailed description of the FEA and each reference model shown above please see <http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html>.

In addition to the architectural domains discussed below, a repeatable development process, producing standard documentation artifacts, has been defined for the NCR DEH. For more information on how to implement an information exchange using these standards and the NCR Exchange Development Life Cycle (EDLC), please see the *NCR Data Exchange Hub Development Toolkit*⁴, found at (<http://www.ncrnet.us/deh/iepd/>).

³ White House, *Federal Enterprise Architecture (FEA)*. Retrieved March 29, 2006 from <http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html>.

⁴ NCR Data Exchange Hub



NCR Interoperability Program

NCR DEH Technology Guidelines

4.1 Data/information guidelines

Data /information guidelines relate to how data exchanges will be defined and structured in a standard way such that additional services can be written to expand their interoperability. The technical guidelines in the following table include both general and specific guidelines. These guidelines, while few, are very powerful so as to add efficiency and interoperability to all NCR data exchange efforts.



NCR Interoperability Program

NCR DEH Technology Guidelines

Table 2. NCR Data Exchange Hub: Architecture Guidelines for Information Domain

No.	NCR Guideline	Description	Reference	Comment/Additional Guidelines
A.1	All schemas and documents will comply with the most current xml standard	The use of xml should be considered a general standard for data exchange in the NCR and in the SOA framework.	W³C XML 1.1 Standard ⁵	Of particular importance is compliance with the W3C specification for ‘well-formed’ xml
1.2	Use NIEM distribution element for all xml-based message distributions. Use (or extend) NIEM resource message (RM for resource information exchange).	A single standard XML foundation for exchanging information between DHS, DOJ, and supporting functions such as Justice, Emergency Management, and Intelligence. NIEM 0.2.1 incorporated the Global Justice Data Exchange Model (GJDXM) and EDXL standards. Provides schemas for many types of information exchanges.	National Information Exchange Model (NIEM): 0.2.1 ⁶	Content of the xml message body should include information sufficient for auditing, verification, and incident reconstruction.
A.3	Develop and document data models, schema groups, and xslt –based example documents to define data exchange.	The public safety community has developed a common set of artifacts to document the structure and content of a NIEM/GJXDM-conformant XML instance used in an information exchange. This is very relevant to the NCR DEH and the NCR, regardless of the specific application.	Information Exchange Package Documentation (IEPD) Guidelines, The Global XML Structure Task Force (XSTF). See NCR Development Toolkit .	The IEP documentation suite will support the development and governance of SLAs for data exchanges.
A.4	Same as above	The public safety community has documented a process for creating data models, NIEM/GJXDM conformant schemas, and instances to define the exchange of data between organizations and jurisdictions.	SEARCH /IJIS Institute Exchange Document Development Process: An Overview ⁷ or see NCR Development Toolkit .	This process is web-service based. It can be used regardless of what public, standard xml model is followed.

⁵ W³C. *Extensible Markup Language 1.1*. Retrieved April 24, 2006 from <http://www.w3.org/XML/>.

⁶ U.S. Department of Homeland Security and U.S. Department of Justice. *National Information Exchange Model 03*. Retrieved April 24, 2006 from <http://niem.gov/tools.php>.

⁷SEARCH. *Exchange Document Development Process: An Overview*. Retrieved April 24, 2006 from <http://www.justiceintegration.com/whitepapers.html>.



NCR Interoperability Program

NCR DEH Technology Guidelines

Other data guidelines that may become appropriate include the following:

- OpenGIS[®] Specifications⁸ from Open Geospatial Consortium (OGC), particularly the following:
 - [OpenGIS[®] Geography Markup Language \(GML\) Encoding Specification 3.1.1](#). To be monitored as efforts proceed to harmonize this standard with the native data structure of the industry –dominant vendor.
 - [OpenGIS[®] Web Services Common Specification 1.0.0](#)⁹.
- Other common, public, and universally accepted xml schema. A variety of standards exist for specific exchange types.
- [Federal Enterprise Architecture Framework \(FEAF\) Data Reference Model \(DRM\)](#)¹⁰: The DRM (version 1.0) is a newly-articulated component of the FEAF that is managed by OMB. It should be considered for a component of any strategy to integrate metadata.
- NCR DEH Metadata Repository.

4.2 Integration/middleware guidelines

Integration/middleware guidelines relate to how web service applications for data exchange will be developed. Much standardization work has been completed so that independently developed services can work together in an interoperable fashion. The technical guidelines in the following table are based on the web services model that is recommended for the NCR DEH. These guidelines are numerous and are independent of any given product or vendor's solution.

⁸ Open Geospatial Consortium. *Geography Markup Language (GML) Encoding Specification 3.1.1*. Retrieved <http://www.opengeospatial.org/specs/?page=specs>.

⁹ Open Geospatial Consortium. *Geography Markup Language (GML) Encoding Specification 3.1.1*. Retrieved <http://www.opengeospatial.org/specs/?page=specs>.

¹⁰ White House, *Federal Enterprise Architecture: Data Reference Model*. Retrieved April 24, 2006 from <http://www.whitehouse.gov/omb/egov/a-5-drm.html>.



NCR Interoperability Program

NCR DEH Technology Guidelines

Table 3. NCR Data Exchange Hub: Architecture Guidelines for Interoperability Middleware Domain

No.	Guideline	Reference	Description	Comment/Additional Guidelines
B.1	Develop web services using standard SOAP envelope, header, and body; WSDL, and UDDI	WS-I Basic Profile 1.1, Web Services Interoperability Organization (WS-I) ¹¹ .	Guidelines for design of Interoperable Web Services. Includes guidelines on use of SOAP , WSDL and UDDI (see below)	Note that current profile endorses UDDI 2.0x. For further information, refer to the NCR Development Toolkit ¹² .
B.2	Use standard form for WSDL for web services, both synchronous and asynchronous.	W³C Web Services Description Language (WSDL) Version 2.0 Specifications ¹³	Standard for developing a WSDL 2.0 document that describes the desired Web service in xml that can easily be transformed into the web service itself. Elements include the following: <ul style="list-style-type: none"> • the kinds of messages that the service will send and receive. • <i>what</i> abstract functionality the Web service provides. • <i>how</i> to access the service. • <i>where</i> to access the service 	
B.3	Process xml documents using xpath standards. Perform content-based routing using xpath standards	W³C xpath 2.0 ¹⁴ Recommendation	A language used to process xml documents. An integral part of standard xslt transformations. Also used for content-based routing	
B.4	Follow standard SOAP conventions in messaging for web	W³C Simple Object Access Protocol (SOAP) 1.1. ¹⁵	A protocol for exchange of information in a decentralized, distributed environment; XML based, consisting of three parts:	.

¹¹ Web Services Interoperability Organization (WS-I). *Basic Profile Version 1.0*. Retrieved April 24, 2006 from <http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html>.

¹² NCR Development Toolkit. Retrieved May 22, 2006 from <http://www.ncrnet.us/deh/toolkit/index.htm>.

¹³ World Wide Web Consortium (W³C). *Web Services Description Language (WSDL) Version 2.0*. Retrieved April 24, 2006 from <http://www.w3.org/TR/wsdl20/>.

¹⁴ Wide Web Consortium (W³C). *XML Path (XMLP) Language 2.0*. Retrieved April 24, 2006 from <http://www.w3.org/TR/xpath20/>.

¹⁵ W³C. *Simple Object Access Protocol (SOAP)*. Retrieved April 24, 2006 from <http://www.w3.org/TR/soap/>.



NCR Interoperability Program

NCR DEH Technology Guidelines

No.	Guideline	Reference	Description	Comment/Additional Guidelines
	services, both synchronous and asynchronous.		<ul style="list-style-type: none"> • an envelope that defines a framework for describing what is in a message and how to process it, • a set of encoding rules for expressing instances of application-defined data types, • a convention for representing remote procedure calls and responses. 	
B.5	Use a service directory to locate and register web service endpoints.	Organization for the Advancement of Structured Information Standards (OASIS) Universal Description, Discovery and Integration (UDDI) 3.0 ¹⁶	A standard for a common service registry to be used by applications look up the location (endpoint URL) of a web service they need to access.	Although UDDI 3.0 supports dynamic, distributed registries, the NCR does not currently endorse that feature as part of the standards. UDDI 3.0 has many other useful features.
B.6	Develop web service policy for data exchanges and attach the assertions to the web service.	WS-Policy, WS-I ¹⁷	A spec for making Web Service policy statements and a mechanism to attach the policy assertions to web services	Policy in web services will be derived as part of NCR DEH governance activities.

¹⁶ OASIS. *Universal Description, Discovery and Integration (UDDI) 3.0*. Retrieved April 24, 2006 from http://uddi.org/pubs/uddi-v3.00_-published-20020719.htm.

¹⁷ Web Services Interoperability Organization. *WS-I Deliverables*. Retrieved April 24, 2006 from <http://www.ws-i.org/deliverables/Default.aspx>.



4.3 Security/privacy guidelines

Security/privacy guidelines relate to how the data and its transporting system (application, network, other infrastructure) can be protected and assured to be reliable, available, and maintainable as needed. The guidelines are wide ranging, covering standard security matters, as well as very specific guidelines for increasing all aspects of assurance in the web service code itself. In addition, there are guidelines on operational best practices. The technical guidelines in the following table are a blend of modern internet protocols, web services specific messaging practices, and 'old school' security controls regarding user ID and passwords. All are necessary components to assure the data and its proper access for the NCR DEH.

The guidelines for operational best practices are included in *Table 5 NCR DEH Security – Related Guidelines to Assure Operational Reliability, Availability and Maintainability*.



NCR Interoperability Program

NCR DEH Technology Guidelines

Table 4. NCR Data Exchange Hub: Architecture Guidelines for Security/Privacy Domain

No.	Guideline	Description	Reference	Comment/Additional Guidelines
C.1	Conduct a security assessment and implement appropriate management, operational, and technical controls	Mandated by the Federal Information Security Management Act (FISMA) of 2002 ¹⁸ , NIST created this publication to provide guidelines on security controls for Federal Information Systems.	National Institute for Standards and Technology SP 800-53 ¹⁹	DEH will implement security controls based on a risk assessment of the system and its interconnections.
C.2	Follow basic security procedures when developing SOAP messages for web service-based data sharing.	Guidelines for design of Interoperable Web Services to minimize vulnerabilities as security objects are passed within the web service software itself.	Web Services Interoperability Organization (WS-I). WS-I Basic Security Profile 1.0 ²⁰	
C.3	Use SOAP security enhancements when sending security tokens.	Addresses SOAP message enhancements for integrity and confidentiality. Guidelines to associate and encrypt security tokens	OASIS Web Services Security v 1.0 (WS-Security 2004) ²¹	Works with a wide range of security products and encryption schemes.
C.4	Use SAML standards for incorporating authentication and authorization information in xml.	Security Assertion Markup Language. Defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.	OASIS SAML 2.0 ²²	DEH will use strong encryption and hashing protocols such as AES and SHA-1.

¹⁸ National Institute of Standards and Technology. *Federal Information Security Management Act (FISMA) of 2002*. Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.

¹⁹ National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems, February 2005*. Retrieved April 24, 2006 from <http://csrc.nist.gov/publications/nistpubs/>.

²⁰ Web Services Interoperability Organization (WS-I). *Basic Profile Version 1.0*. Retrieved April 24, 2006 from <http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html>.

²¹ OASIS. *Web Services Security version 1.0*. Retrieved April 24, 2006 from <http://www.oasis-open.org/specs/index.php#wssv1.0>.

²² OASIS. *Security Assertion Markup Language (SAML)2.0*. Retrieved April 26, 2006 from http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20.



NCR Interoperability Program

NCR DEH Technology Guidelines

No.	Guideline	Description	Reference	Comment/Additional Guidelines
	2.0			
C.5	Use available standards when using security tokens and when trust relationships are established in web services.	There are additional SOAP message enhancements that address issuing, renewing, and validating security tokens and establishing, and brokering trust relationships. Enables secure communication that works with Web services framework, including WSDL service descriptions, UDDI services, and SOAP messages.	WS-I Web Services Trust Language (WS-Trust). Version 1.1	
C.6	Use conventional specifications to maintain security across multiple messages,	This specification defines extensions to WS-Security and WS-Trust to provide secure communication across one or more messages at once. This is especially useful in the NCR for widely distributed messages and for asynchronous web services	WS-Secure Conversation: WS-1	
C.7	Use best practice mechanisms to ensure that SOAP messages properly navigate networks to intended end point.	Mechanisms to address Web services and messages. Defines XML elements to identify Web service endpoints and to secure true origin and destination endpoint identification in messages. This specification enables messages to traverse networks that include endpoint managers, firewalls, and gateways in a transport-neutral manner.	WS-Addressing: W3C (member submission)	
C.8	Develop an x.509 Certificate profile that complies with FPKI guidelines.	Broad guidance and specific metrics for how certificate authorities and authentication is accomplished, both within a government agency (enterprise) and across agencies (federated through a certificate bridge).	Federal PKI Policy Authority X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (Version. 2.4) ²³ March 2006	This will enable integration and interoperation with Federal Government certificate services and applications.
C.9	Encryption and/or digital signature keys shall be at least 2078 bits in length.	Broad guidance and specific metrics for how certificate authorities and authentication is accomplished, both within a government agency (enterprise) and across agencies (federated through a certificate bridge).	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Federal PKI Policy Authority (Version. 2.4), March 2006	The 2048-bit key will become a required standard in 2010.

²³ Federal Public Key Infrastructure (PKI) Policy Authority. *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*. Retrieved April 26, 2006 from <http://www.cio.gov/fpkipa/policies.htm>.



NCR Interoperability Program

NCR DEH Technology Guidelines

No.	Guideline	Description	Reference	Comment/Additional Guidelines
C.10	VPN standards should follow the IPSEC suite, including ISAKMP and ESP protocols.	Internet Security Association and Key Management Protocol (ISAKMP) ²⁴ is a cryptographic protocol that forms the basis of the IKE key exchange protocol. Defined. IPSEC is a mandatory component of IP version 6.	The Internet Society (1998), Network Working Group RFC 2401 ²⁵ , RFC 2408	
C.11	Single sign-on and user authorization should employ LDAP or LDAPS	LDAP, Lightweight Directory Access Protocol, provides a simplified implementation of the x.500 standard for universal directories: names, locations e-mail addressing, user authentication (e.g., logins and passwords), or network security (e.g., user-access rights). LDAPS (LDAP over SSL) is a specialized extension for secure data transmissions.	The Internet Society (1995), Network Working Group RFC 1777 ²⁶	
C.12	Grant access to each user via a static role. The user logs in as an individual, not as a role.	Mandated by the Federal Information Security Management Act (FISMA) of 2002 ²⁷ , NIST created a publication to provide guidelines on security controls for Federal Information Systems.	National Institute for Standards and Technology, SP 800-53 ²⁸ , operational and technical controls	Roles will be collaboratively developed to ensure proper authorization within each role.

²⁴Network Working Group. *Internet Security Association and Key Management Protocol*. Retrieved April 24, 2006 from <http://www.networksorcery.com/enp/protocol/isakmp.htm>.

²⁵ The Internet Society, Network Working Group. *Security Architecture for the Internet Protocol: RFC 2401*. Retrieved April 24, 2006 from <http://rfc.sunsite.dk/rfc/rfc2401.html>.

²⁶ The Internet Society, Network Working Group. *Lightweight Directory Access Protocol: RFC 1777*. (March 1995). Retrieved April 24, 2006 from <http://www.faqs.org/rfcs/rfc1777.html>.

²⁷ National Institute of Standards and Technology. *Federal Information Security Management Act (FISMA) of 2002*. Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.

²⁸ National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*. (Feb 2005). Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.



NCR Interoperability Program

NCR DEH Technology Guidelines

Table 5. NCR Data Exchange Hub: Security – Related Guidelines to Assure Operational Reliability, Availability, And Maintainability

	Guideline	Description	Reference	Comment/Additional guidelines
D.1	Have formal, documented processes for change management, version release and software validation and testing	Standards exist for planning and executing the control and management of software configurations, including builds, releases, forward and backward compatibility, and change control.	IEEE 1042-1987: (Reaff 1993) Software Configuration Management Institute of Electrical and Electronics Engineers	WS-I Basic Profile 1.1 recommends that at least two versions of web service application and interface be supported.
D.2	Failover and load balancing implemented for data sharing servers	Failover, load balancing, and robust backup and recovery procedures are critical to maintaining reliability, availability, and maintainability of operational essential systems.	National Institute for Standards and Technology, SP 800-53²⁹ : Operational controls to assure availability	
D.3	Backup to external system non-removable media	Failover, load balancing, and robust backup and recovery procedures are critical to maintaining reliability, availability, and maintainability of operational essential systems.	National Institute for Standards and Technology, SP 800-53³⁰ : Operational controls to assure availability	
D.4	Backup site operational and receiving real-time synchronizing data	Failover, load balancing, and robust backup and recovery procedures are critical to maintaining reliability, availability, and maintainability of operational essential systems.	National Institute for Standards and Technology, SP 800-53³¹ : Operational controls to assure availability	

²⁹ National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*.(Feb 2005). Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.

³⁰ National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*.(Feb 2005). Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.

³¹ National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*.(Feb 2005). Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.



NCR Interoperability Program

NCR DEH Technology Guidelines

4.3.1 Note on mobile device security

The following guidelines apply when mobile devices, including laptops and Personal Digital Assistants (PDA's) are used to access the NCR DEH:

- Mobile devices must be password protected in accordance with NCR Password policy.
- NCR ESF data should not be stored on unauthorized IT Resources. However, in the event that there is no alternative to local storage, all sensitive/confidential NCR ESF data must be encrypted using approved encryption techniques.
- All remote access to NCR ESF data must be via an Internet Service Provider (ISP) using protocols approved by the NCR.
- Unattended mobile devices and media must be physically secure. This means they must be locked in an emergency vehicle or attached to a desk or cabinet via a cable lock system when not attended.



5 Glossary

CAP	Common Alerting Protocol – An XML-based data format for exchanging emergency alerts and public warnings among different alerting technologies. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, in order to increase warning effectiveness and simplify the warning activation task for responsible officials.
CIO	Chief Information Officer
DHS	Department of Homeland Security
DOJ	Department of Justice
DRM(1)	Digital Rights Management – The umbrella term referring to any of several technical methods used to handle the description, layering, analysis, valuation, trading and monitoring of the rights held over a digital work.
DRM(2)	Data Reference Model – A component of the FEAF (see below) that addresses data storages in cases where XML standards are not applicable.
DTD	Document Type Definitions – Once of several XML schema languages, a set of declarations that conform to a particular markup syntax and that describe a class, or “type” of SGML or XML document, in terms of the constraints on the structure of those documents.
EDXL	Emergency Data Exchange Language – A broad initiative to create an integrated framework for a wide range of emergency data exchange standards to support operations, logistics, planning and finance.
EIA	Electronic Industries Alliance – A trade organization for electronics manufacturers in the U.S. EIA is accredited by ANSI to help develop standards on electronic components, consumer electronics, electronic information, telecommunications, and Internet security.
ESF	Emergency Support Function – A functional area of response activity established to facilitate coordinated delivery of emergency assistance required during the response phase to save lives, protect property and health, and maintain public safety.
FEAF	Federal Government Enterprise Framework – The Clinger-Cohen Act of 1996 mandated that Federal Agencies develop and maintain an enterprise IT architecture. FEAF was established in 1999 by the CIO’s in response to this mandate. The purpose of the FEAF is to facilitate shared development of common processes and information among Federal Agencies and other government agencies.



NCR Interoperability Program

NCR DEH Technology Guidelines

FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards – Publicly announced standards developed by the U.S. Federal government for use by all (non-military) federal government agencies and by government contractors.
GIS	Geographic Information System – A system for creating and managing spatial data and associated attributes.
GJXDM	Global Justice XML Data Model – A data reference model for the exchange of information within the justice and public safety communities. The Global JXDM is a product of the Global Justice Information Sharing Initiative’s (Global) Infrastructure and Standards Working Group (ISWG) and was developed by the Global ISWG’s XML Structure Task Force (XSTF).
GML	Geography Markup Language – The XML grammar defined by the Open Geospatial Consortium (OGC) to express geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet.
HIPAA	Health Insurance Portability and Accountability Act – Enacted by U.S. Congress in 1996 to protect health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers. HIPAA also requires strict privacy of personal health care information.
IEEE	Institute of Electrical and Electronics Engineers – An international non-profit, professional organization for the advancement of technology related to electricity.
IEPD	Information Exchange Package Documentation
ISP	Internet Service Provider
ID-SAFE	Identify Strong Authentication Framework – An open framework to allow strong authentication solutions such as, hardware and software tokens, smart cards, SMS-based systems and biometrics to interoperate across organizations, networks and vertical market segments.
IT	Information Technology – The broad subject concerned with all aspects of managing and processing information.
NCR	National Capital Region – The region surrounding the Washington DC area, including Virginia and Maryland.
NCRIP	National Capital Region Interoperability Program



NCR Interoperability Program

NCR DEH Technology Guidelines

NIEM	National Information Exchange Model – An XML-based standard being adopted by U.S. Federal agencies for the precise exchange of information. NIEM is based on a precisely defined data dictionary that uses ISO-11179 metadata registry standards.
NIMS	National Incident Management System – Developed by the U.S. Secretary of Homeland Security at the request of the President, NIMS integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. NIMS enables responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity.
NIST	National Institute of Standards and Technology – A non regulatory agency of the U.S. Department of Commerce’s Technology Administration. The institute’s mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life.
OASIS	Organization for the Advancement of Structured Information Standards – A global consortium that drives the development, convergence and adoption of e-business and web service standards.
OGC	Open Geospatial Consortium – An international voluntary consensus standards organization. More than 280 commercial, governmental, nonprofit and research organizations worldwide collaborate in an open consensus process encouraging development and implementation of standards for geospatial content and services.
OMB	Office of Management and Budget
ROSS	National Interagency Resource Ordering And Status System – A National Wildfire Coordinating Group (NWCG) sponsored information systems development project. ROSS is a computer software program which automates the resource ordering, status, and reporting process. Established in 1997 and chartered by the NWCG in June 1998, the scope of the project focuses on automating current processes enabling dispatch offices to electronically exchange and track information near real-time. ROSS tracks all tactical, logistical, service and support resources mobilized by the incident dispatch community.
SAML	Security Assertion Markup Language – An XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider.
SDLC	Software Development Life Cycle – A framework for understanding and developing information systems and software successfully.
SDU	Service Data Unit – The payload in an Ethernet frame.
SOA	Service-Oriented Architecture – A software architectural concept that defines the use of services to support the requirements of software



NCR Interoperability Program

NCR DEH Technology Guidelines

	users.
Telematics	The field of electronic navigation and location of mobile objects.
W3C	World Wide Web Consortium – An international consortium where member organizations, a full-time staff, and the public work together to develop standards for the World Wide Web.
WSDLC	Web Services Development Life Cycle
WS-I	An open, industry organization chartered to promote web services interoperability across platforms, operating systems, and programming languages.
UASI	Urban Area Security Initiative – A Federal Homeland Security program designed to fund regional planning and coordination in critical incident response.
UDDI	Universal Description, Discovery, and Integration – A platform-independent, XML-based registry for businesses worldwide to list themselves on the Internet.
VEDS	Vehicular Emergency Data Set – An XML standard for the transmission of Telematics data to emergency response agencies.
XML	Extensible Markup Language – A W3C recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data.
XSTF	The Global XML Structure Task Force



NCR Interoperability Program

NCR DEH Technology Guidelines

Appendix A: References

The following references provide more detail for the concepts in this report.

1. Institute of Electrical and Electronics Engineers. *1512 Standards*[®]. Retrieved April 24, 2006 from <http://grouper.ieee.org/groups/scc32/imwg/>.
2. Kenney, L. Frank, Plummer, Daryl C., & Andrews, Whit (March 9, 2005). *Strengthen your web services framework with the right combination of technologies and products*. Gartner, Inc., G00126007. Retrieved March 24, 2006 from Gartner, Inc. database.
3. National Institute of Standards and Technology. *Federal Information Security Management Act (FISMA) of 2002*. Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.
4. National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*. (Feb 2005). Retrieved April 24, 2006 from <http://csrc.nist.gov/sec-cert/>.
5. Network Working Group. Internet Security Association and Key Management Protocol. Retrieved April 24, 2006 from <http://www.networksorcery.com/enp/protocol/isakmp.htm>.
6. OASIS. *Universal Description, Discovery and Integration (UDDI) 3.0*. Retrieved April 24, 2006 from <http://uddi.org/pubs/uddi-v3.00-published-20020719.htm>.
7. OASIS. *Common Alerting Protocol*. Retrieved April 24, 2006 from <http://www.oasis-open.org/committees/emergency>.
8. Open Geospatial Consortium. *Geography Markup Language (GML) Encoding Specification 3.1.1*. Retrieved <http://www.opengeospatial.org/specs/?page=specs>.
9. SEARCH. *Exchange Document Development Process: An Overview*. Retrieved April 24, 2006 from <http://www.justiceintegration.com/whitepapers.html>.
10. Search Group, Incorporated. (2002) *Justice Information Exchange Model[®] Conceptual Framework*. (2002). Retrieved April 14, 2006, from <http://www.jiem.search.org/JIEMConcepts.pdf>.
11. The Internet Society, Network Working Group. *Security Architecture for the Internet Protocol: RFC 2401*. Retrieved April 24, 2006 from <http://rfc.sunsite.dk/rfc/rfc2401.html>.
12. The Internet Society, Network Working Group. *Lightweight Directory Access Protocol: RFC 1777*. (March 1995). Retrieved April 24, 2006 from <http://www.faqs.org/rfcs/rfc1777.html>.
13. Web Services Interoperability Organization (WS-I). *Basic Profile Version 1.0*. Retrieved April 24, 2006 from <http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html>.
14. White House, *Federal Enterprise Architecture: Data Reference Model*. Retrieved April 24, 2006 from <http://www.whitehouse.gov/omb/egov/a-5-drm.html>.



NCR Interoperability Program

NCR DEH Technology Guidelines

15. White House, *Federal Enterprise Architecture Technical Reference Model*. Retrieved April 24, 2006 from <http://www.whitehouse.gov/omb/egov/a-6-trm.html>.
16. World Wide Web Consortium (W3C). *Extensible Markup Language 1.1*. Retrieved April 24, 2006 from <http://www.google.com/search?hl=en&q=XML+1.1>.
17. World Wide Web Consortium (W3C). *Simple Object Access Protocol (SOAP)*. Retrieved April 24, 2006 from <http://www.w3.org/TR/soap/>.
18. World Wide Web Consortium (W3C). *Web Services Description Language (WSDL) Version 2.0*. Retrieved April 24, 2006 from <http://www.w3.org/TR/wsdl20/>.
19. World Wide Web Consortium (W3C). *XML Path (XMLP) Language 2.0*. Retrieved April 24, 2006 from <http://www.w3.org/TR/xpath20/>.
20. U.S. Department of Homeland Security and U.S. Department of Justice. *National Information Exchange Model 03*. Retrieved April 24, 2006 from <http://niem.gov/>.