



National Capital Region Interoperability Services (NCR-IS)

Information Management Policy v1.0 for distribution

October 2007

**Prepared by the NCR Interoperability Program
Data Exchange Hub Project**

This document was prepared under a grant from the Office of State and Local Government Coordination and preparedness (SLGCP), United States Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of SLGCP or the US DHS.



NCR Interoperability Services (NCR-IS)

Information Management Policy

Executive Summary

The mission of NCR-IS is to enable information sharing and exchanges across the National Capital Region. To ensure a successful outcome, this requires adoption and implementation of an efficient Information Management Policy and accompanying Processes and Procedures. The purpose of this document is to provide policy and regulatory guidance on Information Management in the NCR-IS Architecture.

Information Management is a complex issue and consists of various facets – governance, processes, technology and others. It needs a holistic approach as it is an extensive and lengthy process. Recognizing this, NCR-IS will adopt a phased approach towards the adoption and implementation of a comprehensive Information Management program. In this initial stage, the Policy addresses some of the important areas in the short term; as the evolution towards Data Services matures, this Policy will be updated to address the other areas, and to reflect the input and feedback from NCR-IS Partners. Since the policies vary based on the owner, and to emphasize the ownership attributes of data, this Policy classifies data into the following logical categories:

- NCR-IS Partner Data – data owned by the NCR-IS Partners
- NCR-IS Data - data owned by NCR-IS, including the metadata that is collected on the assets, such as hardware, and entities, such as organizations and data exchanges, in the NCR-IS environment. It may also include data that is hosted by NCR-IS on behalf of NCR-IS Partners.

Efficient Information Management requires availability of skilled resources and this policy recognizes that NCR-IS and NCR-IS Partners require skilled resources, with certain roles and responsibilities, to ensure effective management of Information in the NCR-IS Environment.

Role of NCR-IS

NCR-IS will serve as a data custodian (see NCR-IS Glossary of Terms, Roles and Position v1) for all data assets provided by the NCR-IS Partners. As mentioned above, it will serve as an intermediary for information exchanges. NCR-IS will not edit, transform or make changes to the content of the partner data unless authorized by NCR-IS Partners. NCR-IS will be the owner of metadata that is collected .

Overview of Policies

The section below highlights some of the policies and the reader is advised to see the NCR-IS Information Management Policy for the complete list of policies and their descriptions.

- Ownership of the data will remain with the NCR-IS Partner that provided the data.
- Once data is submitted to NCR-IS, it will act as a Custodian of the data.
- NCR-IS Partners will identify the business rules for each data element or classes of data that they provide.
- NCR-IS Partners will be responsible for the quality of the data – to the best of their ability - provided to NCR-IS.

This Policy refers to the IT Service Management Framework and NCR-IS Security Policy v1 for issues of Change Management and Information Security.



Table of Contents

1	PURPOSE	1
2	GOALS AND OBJECTIVES	1
2.1	GOALS	1
2.2	OBJECTIVES	1
3	SCOPE	2
3.1	RELATED WORK	2
4	DATA GOVERNANCE	2
4.1	STRUCTURE	2
4.1.1	<i>Data Classification</i>	2
4.2	ROLES AND RESPONSIBILITIES	3
4.3	ROLE OF NCR-IS	3
5	POLICIES	3
5.1	BUSINESS RULES	4
5.2	DATA OWNERSHIP	4
5.3	DATA SHARING	4
5.4	DATA STORAGE	5
5.5	DATA QUALITY	5
5.6	METADATA MANAGEMENT	6
5.7	DATA STANDARDS	6
5.8	IT SUPPORT PROCESSES	7
5.9	INFORMATION SECURITY	7
5.10	INDEMNIFICATION	7
	APPENDIX A: METADATA IN THE NCR-IS ENVIRONMENT	8
	APPENDIX B: GLOSSARY OF TERMS, ROLES AND POSITIONS	9
	APPENDIX B1: GLOSSARY OF TERMS	9
	APPENDIX B2: GLOSSARY OF ROLES - NCR-IS CENTRAL ROLES	16
	APPENDIX B3: GLOSSARY OF ROLES - NCR-IS PARTNER ROLES	19
	APPENDIX B4: GLOSSARY OF ROLES - SERVICES AND RELATED SUPPORT ROLES	21
	APPENDIX C: REFERENCES	23

List of Figures

<i>Figure 1. Matrix of Services and Related Support Roles</i>	22
---	----



NCR Interoperability Services (NCR-IS)

Information Management Policy

1 Purpose

The mission of National Capital Region Interoperability Services (NCR-IS) entity is to enable information sharing and exchanges across the NCR. To ensure a successful outcome, this requires adoption and implementation of an efficient Information Management Policy and accompanying processes and procedures. The purpose of this document is to provide policy and regulatory guidance on information management in the NCR-IS Architecture.¹

2 Goals and Objectives

2.1 Goals

The primary goal of the Information Management domain is to support the business, technical and Service Management capabilities provided by the NCR-IS. To enable this, the data in the NCR-IS environment needs to be²:

- Visible
- Accessible
- Interoperable
- Trusted.

Information Management is a complex issue and consists of various facets – governance, processes, technology and others. It needs a holistic approach as it is an extensive and lengthy process. Recognizing this, NCR-IS will adopt a phased approach towards adopting and implementing a comprehensive Information Management program. This document is an initial step in this multi-level iterative process. Further revisions will expand on the areas listed in the document. In addition, they will include and address the other critical areas like – Knowledge Management, Spatial Data Management, Data Lifecycle Management, Data Federation, and others. In the long term, Information Management will be a fundamental and integral component of Data Services – services that perform data integration functions - offered by NCR-IS.

2.2 Objectives

In particular, the Information Management domain supports the following objectives from the NCR Data Exchange Hub Data Sharing and Security Strategy.³

- Objective 1 – Ensure device independent access to data and services in real time when needed through implementation of a Services Oriented Architecture.
- Objective 3 – Develop, adopt, and implement standard policies, processes and procedures to facilitate information sharing.

¹ For the purposes of this document Information Management includes Data and Metadata Management, and Data Integration.

² Federal Enterprise Architecture DRM Data Management Strategy DRAFT, February 2004.

³ NCR Data Exchange Data Sharing and Security Strategy, June 2006.



NCR Interoperability Services (NCR-IS)

Information Management Policy

3 Scope

The scope of this document is limited to identification of the data and metadata management policies for National Capitol Region Interoperability Services (NCR-IS). It addresses the business rules, data ownership, data storage, data sharing, metadata management, and data quality.

It includes all participating organizations and agencies that provide, manipulate, or use the information services of the NCR-IS.

3.1 Related Work

This document refers to the following documents:

- NCR-IS Security Policy Version 1
- NCR-IS Service Management Framework Version 1
- NCR-IS Service Management Service Catalog Version 1.

4 Data Governance

The policies in this document are recommended by the Metropolitan Washington Council of Governments (MWCOG) Chief Information Officers (CIO) Architectural Review Committee (ARC), vetted by the MWCOG CIO Committee, and formerly adopted by the Chief Administrative Officers (CAO) Committee. Policies will be enforced by a Governance and/or Oversight Board, resulting from the governance definition effort currently being undertaken by the MWCOG CIO committee.

4.1 Structure

4.1.1 Data Classification

4.1.1.1 NCR-IS Partner Data

NCR-IS Partner Data is defined as the data that is owned by the NCR-IS Partners. There will be a single primary owner assigned to each data stream by each Partner.

4.1.1.2 NCR-IS Data

NCR-IS Data is data owned by NCR-IS, and will include metadata that is collected and archived. Metadata may be collected on assets, such as hardware and software for Configuration Management purposes. Please refer to the NCR-IS Service Catalog which defines IT Support Processes including Configuration, Change, Release, Incident and Availability Management.

It will also include metadata collected on entities, such as organizations and data exchanges. In addition, it will include derived data. (See NCR-IS (previously NCR_DEH) Consolidated Requirements document).



NCR Interoperability Services (NCR-IS)

Information Management Policy

4.1.1.3 Non-Partner Data

In addition, there may be other sources of data who may be non-partners of NCR-IS – for example: private industry, federal government etc.

4.2 Roles and Responsibilities

Efficient Information Management requires availability of skilled resources and this policy recognizes that NCR-IS and NCR-IS Partners require skilled resources, with certain roles and responsibilities, to ensure effective management of Information in the NCR-IS Environment. Furthermore, regulatory or legislative guidance and mandates may require the addition or modification of certain roles and responsibilities, if any, in the future.

Please refer to the NCR-IS Glossary of Terms, Roles and Positions in Appendix B for a list of NCR-IS and NCR-IS Partner roles relevant to Data Management.

4.3 Role of NCR-IS

NCR-IS will serve as a data custodian for all data assets provided by the NCR-IS Partners. As mentioned above, it will serve as an intermediary for information exchanges and will not be responsible for the accuracy, integrity or consistency of the original data that was provided to it. But, it will ensure to *maintain* the accuracy and integrity of the data, as provided, during the transaction and when the data is the NCR-IS environment.

NCR-IS will not edit, transform or make changes to the content of the partner data. It may be necessary to modify the format of the partner data which may be done after obtaining authorization from the partners. Any such necessary actions will be declared in the Information Exchange Packet Documentation (IEPD) artifacts. The integrity of the data will be the responsibility of the jurisdiction.

NCR-IS will be the owner of metadata that is collected and archived. It will be responsible for the accuracy, integrity, security and privacy this metadata that is collected and will ensure the quality of this metadata.

NCR-IS may also serve as owner of data where NCR-IS Partners have conferred joint ownership for the purposes of dissemination of data – such as training material, directories, or public information – to the NCR-IS Partners or the general public.

Finally, NCR-IS may create and provide derivative works from the collected data and metadata. These functions may include data analysis, reporting on certain data attributes, and others.

5 Policies

This section addresses the policies for the data and metadata management in the NCR-IS Environment. It addresses the business rules, data ownership, data storage, data sharing, metadata management, and data quality.



NCR Interoperability Services (NCR-IS)

Information Management Policy

NCR-IS will review and make updates to this Information Management Policy based on changes in technology or operations, or other valid reasons. Any changes will be vetted by the ARC and validated by the COG CIO Governance committee and disseminated to the NCR-IS partners.

5.1 Business Rules

- 5.1.1** NCR-IS Partners will identify the business rules for each data asset/s that they provide. These business rules will be documented in the Service Level Agreement (SLA) which will accompany each exchange.
- 5.1.2** NCR-IS Partners will ensure that the business rules identified include the federal, state, or local policies, regulations, or standards that the partner is already observing in regard to the data element or classes of data provided.
- 5.1.3** NCR-IS will ensure that the business rules are enforced when the data is in the NCR-IS environment.

5.2 Data Ownership

- 5.2.1** Each NCR-IS Partner i.e. jurisdiction shall, at a minimum, identify a Data Owner and Data Steward for each data asset that is involved in a data exchange with NCR-IS (See the NCR-IS Glossary of Terms, Roles and Positions v1).⁴
- 5.2.2** Ownership of the data will remain with the NCR-IS Partner that provided the data. Once data is submitted to NCR-IS, it will act as a Custodian of the data.
- 5.2.3** For the purpose of sharing data of general use to all NCR-IS Partners, a partner may elect to confer joint ownership of data to NCR-IS.

5.3 Data Sharing

- 5.3.1** NCR-IS will work with each individual NCR-IS Partner to develop and identify data access and sharing patterns – it will work with each individual NCR-IS Partner to identify how data will be accessed by NCR-IS or how data will be provided to NCR-IS.
- 5.3.2** For exchanges, Information Exchange Packet Documentation (IEPD) and its associated artifacts will be developed as part of the NCR Exchange Development Life Cycle (EDLC) and provided by NCR-IS.⁵

⁴ A key aspect in a multi-stakeholder environment is data ownership and clear identification of the data owner and the role of the other stakeholders. This policy emphasizes that the ownership and control of their data lies with NCR-IS partners, NCR-IS and other agencies are authorized custodians for the duration of the business process/information exchange.

⁵ NCR Exchange Development Life Cycle (EDLC), June 2006.



NCR Interoperability Services (NCR-IS)

Information Management Policy

- 5.3.3** Information exchanges and sharing between NCR-IS and Partners, and among themselves will be governed by the Service Level Agreements (SLAs). See Sample (TBD)
- 5.3.4** NCR-IS and its Partners will ensure compliance and support of Requirements as identified in the NCR-IS (previously NCR_DEH) Consolidated Requirements document.⁶
- 5.3.5** NCR-IS and NCR-IS Partners shall ensure the continued availability of data
- 5.3.6** NCR-IS Partners shall enforce the use of a Memoranda of Understanding (MOU) and a Service Level Agreement (SLA).

5.4 Data Storage

- 5.4.1** The majority of data, stored in NCR-IS Architecture – relates to Derived Data (See NCR-IS (previously NCR_DEH) Consolidated Requirements document.⁷) and CMDB metadata. (See Appendix C)
- 5.4.2** While the goal of NCR-IS is not to store NCR-IS Partner data, it may be necessary at times, to cache (see glossary for a definition) data for some period of time. In such circumstances, the conditions and other parameters – agreed to by the NCR-IS Partners - will be documented in the SLA which will accompany each exchange.
- 5.4.2** NCR-IS Partners who wish to share data with other jurisdictions – such as training videos, planning or documentation – may request that NCR-IS store such data by conferring joint ownership to NCR-IS.
- 5.4.3** NCR-IS Partners who confer ownership to NCR-IS for shared data will provide criteria of consumption of such data to NCR-IS.
- 5.4.4** NCR-IS will store and archive metadata which will be used for better data management and utilization, and for auditing and reporting capabilities.
- 5.4.5** NCR-IS will manage the databases in the NCR-IS architecture and ensure that data management procedures are followed.
- 5.4.6** NCR-IS will validate and check the quality before data/metadata is stored or archived.

5.5 Data Quality

- 5.5.1** NCR-IS Partners will ensure the quality of the data to the best of their ability, and with appropriate disclaimers associated, provided to NCR-IS.⁸

⁶ NCR DEH Technical Requirements, June 2006.

⁷ NCR DEH Technical Requirements, June 2006.

⁸ Data Quality is a significant issue that many organizations are struggling with. NCR-IS envisions that in the initial stages, the data quality and the processes associated, will not be optimal. So, the initial data quality assessments and metrics will be simple, and will evolve as data quality across the NCR-IS environment matures.



NCR Interoperability Services (NCR-IS)

Information Management Policy

- 5.5.2** NCR-IS Partners shall ensure the integrity of data up to their point of demarcation as defined in an MOU and/or SLA.
- 5.5.3** NCR-IS Partners shall ensure that data submitted to the NCR-IS reflects the value of data at the source.⁹
- 5.5.4** NCR-IS will, if requested by NCR-IS Partner, provide – based on the desired level of data quality provided by the NCR-IS Partner – business rules for data correction and synchronization to ensure continued Data Quality.

5.6 Metadata Management

- 5.6.1** NCR-IS will be the *Data Owner* of the metadata that is collected and archived and will ensure the security and privacy of metadata. Permission to externally distribute this metadata will require the consent of all contributing NCR-IS Partners.
- 5.6.2** NCR-IS will collect metadata by using either an automated/machine-generated or manual process. As much as possible, NCR-IS will ensure that the metadata is machine-generated.
- 5.6.3** NCR-IS will provide a mechanism for the NCR-IS Partners to submit metadata manually or edit the captured metadata through automated means.
- 5.6.4** NCR-IS – with NCR-IS Partners - will identify the metadata needs for the entities describing the data exchange and will provide template/s for NCR-IS Partners to use to ensure a consistent standard and format.
- 5.6.5** NCR-IS will provide a template for mapping the partner data to an agreed upon data standard to support the exchange.
- 5.6.5** The metadata will be stored in a repository – in the distributed and redundant DEH architecture - and authorized NCR-IS Users and authorized NCR-IS Partner users will be able to view and query the metadata assets in the NCR-IS environment.
- 5.6.6** NCR-IS will ensure that the metadata will be available and accessible to the NCR-IS Partners.
- 5.6.7** If NCR-IS Partners download/use the metadata, they will comply with the usage policies.

5.7 Data Standards

- 5.7.1** Where applicable, the NCR-IS will use open standards for data and metadata in the NCR-IS environment (see Appendix A for definition of metadata). For more

⁹ NCR-IS or NCR-IS Partners will not be responsible for any liability due to the defects or inaccuracies in the data provided. NCR-IS Consuming Partners shall validate the data before its use.



NCR Interoperability Services (NCR-IS)

Information Management Policy

information on standards refer the [NCR DEH Technology Guidelines](#) published in June 2006.¹⁰

5.8 IT Support Processes

Please refer to the NCR-IS Service Catalog which defines IT Support Processes including Configuration, Change, Release, Incident and Availability Management.

5.9 Information Security

The NCR-IS Security Policy v1 will address the following:

- Security Classification for Data and Metadata Access
- Role-based access and authorization structure
- Security Policies and procedures, including backup, recovery and compliance.
- Auditing and Reporting.

Note: Refer to the NCR-IS Security Policy Document for the security-related policies on data.

5.10 Indemnification

This topic will be addressed in supporting NCR-IS documents relating to Governance.

¹⁰ NCR Data Exchange Hub Technology Guidelines, June 2006.



Appendix A: Metadata in the NCR-IS Environment

Metadata collection and analysis provides a number of benefits and NCR-IS will collect metadata, to ensure better data management and data quality processes in the NCR-IS environment.

The collection and analysis of metadata will provide the following benefits to NCR-IS:

- Managed utilization of resources
- Improved understanding of overlaps in Emergency Support Functions.
- Better management decisions
- Improved ability to perform impact analysis of unavailable assets.

NCR-IS will adopt an evolutionary approach to collect and track metadata. The metadata to be collected will be described in an overall metamodel. In the short term, the focus will be on those metadata elements that are critical to its operations and support. NCR-IS will collect the following types of metadata:

- Administrative (i.e., organization name)
- Business Metadata (i.e., Data Owner name)
- Technical (i.e., server IP address database table names).

The sources for metadata will include the following:

- Databases
- Files
- Paper documents
- Electronic inventory processes
- Data models
- Personnel knowledge.



Appendix B: Glossary of Terms, Roles and Positions

Appendix B1: Glossary of Terms

Cache The act of buffering data to memory or hard disk to optimize access to frequently accessed information. The buffered data is routinely emptied from temporary storage on a pre-defined schedule, or as new information is loaded to replace old data.

Example: In the case of NCR-IS, information from jurisdictions determined to be accessed or updated frequently shall be cached on the NCR-IS XML Server. Based on the SLA for the data exchange controlling the information, the cache shall be cleared or refreshed on a pre-defined basis.

Capital Wireless Integrated Network (CapWIN) A program which allows data sharing, incident management and coordination among public safety agencies in Maryland, Washington D.C., and Virginia.

Configuration Item (CI) Component of an infrastructure - or an item, such as a Request for Change, associated with an infrastructure - that is (or is to be) under the control of Configuration Management. CIs may vary widely in complexity, size and type, from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component.

Configuration Management (CM) The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items and Requests For Change, and verifying the completeness and correctness of Configuration Items.

CONPLAN The U.S. Government Interagency Domestic Terrorism Concept of Operations Plan. The CONPLAN was designed to provide overall guidance to Federal, state, and local agencies concerning how the Federal government would respond to a potential or actual terrorist threat or incident, particularly one involving weapons of mass destruction (WMD). The CONPLAN was created to implement Presidential Decision Directive 39 (1995), which sets forth U.S. policy on counter-terrorism and includes six Federal agencies as signatories to the plan: Department of Justice, Federal Emergency Management Agency, Environmental Protection Agency, Department of Energy, Department of Defense, and the Department of Health and Human Services.

Consequence Management Measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise primary authority to respond to the consequences of terrorism (source: Federal Response Plan Terrorism Incident Annex, page TI-2, April 1999).

Contingency Plan (CP) A document setting out an organized, planned, and coordinated course of action to be followed which targets a specific issue or event that arises during the course of disaster operations and presents alternative actions to respond to the situation.

Council of Governments (COG) The Metropolitan Washington COG is a regional organization of 19 Washington metropolitan area local governments surrounding the Nation's capital, plus area members of the Maryland and Virginia legislatures, the U.S. Senate, and the U.S. House of Representatives.



NCR Interoperability Services (NCR-IS)

Information Management Policy

Crisis Management Predominantly a law enforcement function that includes measures to identify, acquire, and plan the resources needed to anticipate, prevent, and/or resolve a threat of terrorism. The FBI is the LFA for crisis management for such an incident (source: FBI).

During crisis management, the FBI coordinates closely with local law enforcement authorities to provide successful law enforcement resolution to the incident. The FBI also coordinates with other Federal authorities, including FEMA (source: FRP Terrorism Incident Annex, April 1999).

Critical Incident An incident is deemed critical if when a problem occurs vital information is interrupted from reaching the desired destination in an expedient manner as required. The type of information exchange in this type of incident has the requirements of being delivered in a real-time or near real-time manner. Therefore, support for this type of incident will be handled in accordance with the Performance Standards listed for that particular service.

Critical Infrastructure is a term used by governments to describe material assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for ;electricity generation and distribution; telecommunication; water supply; agriculture, food production and distribution; heating (natural gas, fuel oil); public health; transportation systems (fuel supply, railway network, airports); financial services and security services (police, military).

Data is a value, or set of values representing a specific concept or concepts. Data becomes "information" when analyzed and possibly combined with other data in order to extract meaning, and to provide context. The meaning of data can vary according to its context (DRM usage).

Data Accuracy The extent to which data is correct and reliable (Free-of-Error).¹¹

Data Artifact A collective term for electronic objects or artifacts related to the presentation, description, representation, or storage of data. Examples are documents and XML Schemas.

Data Asset The name of a managed container for data; examples include a relational database, Web site, document repository, directory or data service; (DRM usage).

Data Completeness The extent to which data is not missing and is of sufficient breadth and depth for the task at hand (source: Federal Enterprise Architecture DRM).

Note: In the context of NCR-IS, this means the completeness of data provided by the partners to satisfy the information exchange.

Data Consistency The extent to which data is presented in the same format (source: Federal Enterprise Architecture DRM).

Data Integrity The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner; (RFC2828, Internet Security Glossary).

Data Management Principles, processes, and systems for the sharing and management of data (CMMI V1.1).

Data Owner The data owner is the primary owner of the data and all authority of the data rests with the data owner. The Data Owner is responsible to update the data as required, and is responsible for the creation, collection dissemination and maintenance of qualified, accurate, and

¹¹ Federal Enterprise Architecture Data Reference Model (DRM) Version 2.0 (November 17, 2005). Retrieved from <http://www.whitehouse.gov/omb/egov/a-5-drm.html>.



NCR Interoperability Services (NCR-IS)

Information Management Policy

timely data content; ensuring the cleanliness of data prior to submission to the NCR-IS; and provides timely notification to subscribers when the integrity of information is in question.

Data Stewardship Identifying, defining, specifying, sourcing, and standardizing data assets across all business areas within a specific business subject area consisting of some set of entity types, e.g., person.

Data Service Data Service is the name of a process to include all software that performs a data integration task.

Emergency As defined in the Stafford Act, an emergency is any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property, public health, and safety, and includes emergencies other than natural disasters.

Emergency Alert System (EAS) A system established by the FCC in November of 1994 to replace the Emergency Broadcast System (EBS) as a tool the President and others might use to warn the public about emergency situations.

Emergency Broadcast System (EBS) A system replaced by the EAS that was composed of AM, FM, and TV broadcast stations; low-power TV stations; and non-government industry entities operating on a voluntary, organized basis during emergencies at national, state, or operational (local) area levels.

Emergency Operations Center (EOC) is any designated secure location to determine situational status, coordinate actions, and make critical decisions during emergency and disaster situations.

Federal Emergency Management Agency (FEMA) The designated lead Federal agency (LFA) for consequence management to ensure that the Federal Response Plan is adequate to respond to terrorism. Additionally, FEMA supports the Federal Bureau of Investigation (FBI) in crisis management.

Federal Response Plan (FRP) The FRP establishes a process and structure for the systematic, coordinated, and effective delivery of Federal assistance to address the consequences of any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S. Code [USC], et seq.). The FRP Terrorism Incident Annex defines the organizational structures used to coordinate crisis management with consequence management (source: FRP Terrorism Incident Annex, April 1999).

Freedom of Information Act (FOIA) The implementation of freedom of information legislation in the United States was signed into law by President Lyndon B. Johnson on July 4, 1966, and went into effect the following year.

Health Insurance Portability and Accountability Act (HIPAA) Also known as the "Kennedy-Kassebaum Act," this U.S. law (Public Law 104-191) of 1996 protects employees' health insurance coverage when they change or lose their jobs (Title I) and provides standards for patient health, administrative and financial data interchange (Title II). The latter also governs the privacy and security of health information records and transactions. HIPAA took effect in 2001 with compliance required in phases up to 2004 (www.cms.hhs.gov/hipaa).

Homeland Security A concerted national effort to prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and minimize the damage and recovery from attacks that do occur (National Strategy for Homeland Security, 2002).



NCR Interoperability Services (NCR-IS)

Information Management Policy

Homeland Security Information Network (HSIN) HSIN Critical Infrastructure Pilot is an unclassified network and governance program providing a nation-wide platform that enables the sharing of essential homeland security information with the proper stakeholders. This information sharing is accomplished both horizontally across the government and vertically among federal, state and local governments, private sector and citizens as outlined in the President's National Strategy for Homeland Security.

Information Technology Infrastructure Library (ITIL) This is a customizable framework of best practices that promote quality computing services in the IT industry. ITIL addresses the organizational structure and skill requirements for an IT organization by presenting a comprehensive set of management procedures with which an organization can manage its IT operations.

Information Management includes the use of a document and hierarchical information management system. The process ensures that the right information is stored in the appropriate media, with the right level of access and speed of retrieval. Information Management domain supports the following objectives from the NCR Data Exchange Hub Data Sharing and Security Strategy: Ensure device independent access to data and services in real time when needed through implementation of a Services Oriented Architecture; and develop, adopt, and implement standard policies, processes and procedures to facilitate information sharing.

Infrastructure A set of interconnected structural elements that provide the supporting framework of entire structure. The meaning of infrastructure often includes the concept that infrastructure provides organizing structure and support for the system or organization it serves, whether it is a city, a nation, or a corporation.

Incident Command System (ICS) A model for disaster response that calls for the use of common terminology, modular organization, integrated communications, unified command structure, action planning, manageable span-of-control, pre-designated facilities, and comprehensive resource management.

Institutional Network (INET) see definition for NCRnet.

Major Disaster, as defined under the Stafford Act, any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Memorandum of Agreement (MOA) or cooperative agreement is a document written between parties to cooperatively work together on an agreed upon project or meet an agreed upon objective. The purpose of an MOA is to have a written understanding of the agreement between parties. The MOA can also be a legal document that is binding and hold the parties responsible to their commitment or just a partnership agreement.

Memorandum of Understanding (MOU) is a legal document describing an agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. It is a more formal alternative to a gentlemen's agreement, but generally lacks the binding power of a contract.



NCR Interoperability Services (NCR-IS)

Information Management Policy

Metadata is information regarding the characteristics of any artifact, such as its name, location, quality and value to the enterprise and its relationship to other artifacts that an enterprise has deemed worth managing.

Mitigation Those actions, to include threat and vulnerability assessments, taken to reduce the exposure to and detrimental effects of a Weapons of Mass Destruction (WMD) incident.

Mutual Aid Agreement is a written agreement between agencies, organizations, and/or jurisdictions to assist in times of need by furnishing personnel, equipment, and expertise in a specified manner. An agency must first commit its own resources prior to asking for assistance.

NCR-IS Architecture consists of the infrastructure, applications, information and services deployed to achieve the NCR-IS mission.

NCR-IS Data is data owned by NCR-IS, and will include metadata that is collected and archived. Metadata may be collected on assets, such as hardware and software. It will also include metadata collected on entities, such as organizations and data exchanges. In addition, it will include Derived Data (See NCR-IS (previously NCR_DEH) Consolidated Requirements document.

NCR-IS Demarcation The point within the NCR-IS Architecture at which a jurisdiction's responsibility ends. Demarcation points are clearly defined in the MOU, Interconnection Agreements and SLAs.

National Capital Region Network (NCRnet) An NCR Interoperability Program intended to offer optical, high speed, resilient networking capabilities to NCR partner jurisdictions.

NCR-IS Partner Data NCR-IS Partner Data is defined as the data that is owned by the NCR-IS Partner. There will be a single primary owner of this data.

NCR-IS Partner System Any system component owned by an NCR-IS Partner providing some service or set of functionality to the NCR-IS.

NCR-IS Program Defined as the management and organizational structure of the NCR-IS Architecture, the NCR-IS Architecture Program is responsible for setting forth policy related to the NCR-IS Architecture Service.

NCR-IS Operational Environment The organization, human resources and operational resources of the NCR-IS.

NCR-IS Service is defined as a technical web service that can be provided or consumed according to standard Web service protocols (i.e., SOAP, WSDL, UDDI). NCR-IS Web Services facilitate data exchange and system interoperability by providing common system routines that can be used by various NCR-IS Partners' applications across ESFs and jurisdictions.

National Information Exchange Model (NIEM) is an XML-based metadata registry being adopted by U.S. Federal agencies for the exchange of information. NIEM is based on a precisely defined data dictionary that uses ISO/IEC 11179 metadata registry standards.

Non-Critical Incident In this type of incident, any problem or issues that occur do not have an affect on other parties outside the reporting party or does not impede the exchange of information whether critical or not. Therefore, support for this type of incident will be handled in accordance with the Performance Standards listed for that particular service.

Organization for the Advancement of Structured Information Standards (OASIS) Founded in 1993 OASIS is a not-for-profit, global consortium that contributes to the development,



NCR Interoperability Services (NCR-IS)

Information Management Policy

convergence and adoption of web services, e-business and security standards in the public sector and for application-specific markets.

Preparedness A continuing process which establishes the plans, training, exercises, and resources necessary to achieve readiness for all hazards, including WMD incidents.

Professional Services The value added activities that IT staff provide in order to support, maintain, monitor or ensure the consistent and reliable delivery of the technical services.

Public Safety Wireless Network (PSWN) Joint Department of Justice and Department of Treasury program that promotes Federal and local government communications interoperability and sponsors innovative pilot projects.

Satellite-Based Technology Communication systems that are not prone to the same outages as terrestrially based systems.

Release Management (RM) is the process of managing new and/or changed CI's which are tested and introduced into the live environment together.

Regional Wireless Broadband Network (RWBN) Regional Wireless Broadband Network (RWBN) is a seamless interoperable, wireless broadband network of networks with the capacity to provide integrated voice, video and data solutions for public safety agencies leveraging standardized commercially available technologies as well as dedicated public safety frequencies.

Shelter in Place To stay where one is in the event of an emergency. A Shelter in Place requires that people stay inside a building away from windows. All windows and air intake systems should be closed. Wet towels or tape may be used to seal cracks. If there is a danger of explosion windows should be covered.

Sensitive But Unclassified (SBU) Information defined as that which does not meet standards of classification but requires confidentiality to safeguard from public disclosure.

Service Delivery is defined as the delivery of one or more services which enable a business process.

Service Level Agreement (SLA) A formal written agreement between the service provider, NCR-IS Architecture, and the service recipient, the NCR-IS Partner that documents agreed service levels for a service. It is a core concept of IT Service Management. The SLA itself defines the basis of understanding between the two parties for delivery of the service itself. The SLA sometimes underpins a formal contract. The contents will vary according to the nature of the service itself, but usually includes a number of core elements, or clauses.

Service Management is the management of services to meet the Customer's requirements.

Technical Services A technology based capability that the customer consumes or uses in order to facilitate a business process or function.

Terrorism The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Domestic terrorism involves groups or individuals who are based and operate entirely within the United States and U.S. territories without foreign direction and whose acts are directed at elements of the U.S. government or population.

Weapons of Mass Destruction (WMD) Any explosive, incendiary, or poison gas; bomb, grenade, rocket having a propellant charge of more than 4 ounces; missile having an explosive incendiary charge of more than 0.25 ounce; mine or device similar to the above; weapon



NCR Interoperability Services (NCR-IS)

Information Management Policy

involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life (source: 18 USC 2332a as referenced in 18 USC 921).



NCR Interoperability Services (NCR-IS)

Information Management Policy

Appendix B2: Glossary of Roles - NCR-IS Central Roles

The following terms and descriptions represent roles and responsibilities applicable to personnel involved with the design and operation of the NCR-IS organization, its systems and services.

The **NCR-IS Agency Head** is ultimately responsible for fulfilling the NCR-IS mission for the development and implementation of the agency functions and enabling capabilities. The Agency Head is also responsible for ensuring that all agency information technology resources, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation, policy and standards.

The **NCR-IS Chief Information Officer (CIO)** shall ensure organizational compliance with laws and regulations. Establish and adopt NCRIS strategies. Ensure their respective NCRIS component is properly resourced and budgeted for using industry accepted Capital Planning and Investment Control (CPIC) processes. Provide a program management capability to fulfill requirements; maintain policies, practices, and procedures; and ensure the effective operation of programs. Monitor program performance using industry accepted Value Measurement Methodologies (VMM) and ensure continuous performance reporting.

The **NCR-IS Chief Technology Officer (CTO)** shall maintain and staff a centralized security function to implement and control the Information Technology Security Program. The Director of DIT/CTO will appoint a NCR-IS Architecture Security Officer to lead this function.

The **NCR-IS Auditor** validates the integrity of policies, processes and procedures; ensures proper implementation of security controls; reviews logs and records to ensure data has not been altered, omitted, or unlawfully constructed. The NCR-IS Auditor performs routine inspections of NCR-IS Partner Data to ensure compliance with NCR-IS governance as well as document and submit findings to the NCR-IS Custodian and NCR-IS CIO's.

The **NCR-IS Authorizing Official (AO)** is a designated official who is responsible for operating the NCR-IS Architecture at an acceptable level of risk to agency operations, assets, or individuals. The NCR-IS AO has the authority to issue an Interim Authorization To Operate (IATO) for the NCR-IS Architecture under specific terms and conditions and can deny authorization to operate or halt operations of the NCR-IS Architecture if unacceptable security risks exist. The NCR-IS AO interacts with the NCR-IS Senior Agency Information Security Officer (SAISO), Information System Owner (ISO), and NCR-IS Information System Security Officer, Certification Agent, and User representative(s).

The **NCR-IS Senior Agency Information Security Officer (SAISO)** will possess professional qualifications, including training and experience, required to administer the information security functions of the NCR-IS Architecture. The NCR-IS SAISO is primarily responsible for implementing existing and converging security policies as defined by national, state, local government, and organizational policies. The NCR-IS SAISO reports to the NCR-IS AO on matters relative to the security operations of the NCR-IS Architecture. Additionally, the NCR-IS SAISO serves as a liaison to the NCR-IS Information System Owner (ISO), and NCR-IS Information System Security officers (ISSO).

The **NCR-IS Certification Agent (CA)** is responsible for providing full and accurate assessments of the NCR-IS Architecture management, operational and technical security controls and reporting of the state of such controls to the NCR-IS SAISO. It performs this role in an independent manner from NCR-IS operations, maintenance, or management. In instances where it



NCR Interoperability Services (NCR-IS)

Information Management Policy

has been determined that there are vulnerabilities, the NCR-IS CA provides recommended corrective actions to reduce or eliminate such vulnerabilities. The NCR-IS Certification Agent shall also ensure the integrity of implemented security controls by conducting Security Test and Evaluation (ST&E) testing.

The **NCR-IS Information System Owner (ISO)** is responsible for the overall procurement, development, integration, modification, or operation and maintenance of the NCR-IS Architecture; development and maintenance of the system security plan (SSP); and deployment and operation, according to the agreed-upon security requirements. The NCR-IS ISO shall maintain responsibility for determining who has access to the NCR-IS Architecture (including types of privileges and access rights); ensuring that system users and support personnel receive the requisite security training; and maintain responsibility for performing risk assessment activities.

The **NCR-IS Information System Security Officer (ISSO)** is responsible to the NCR-IS AO, NCR-IS ISO, or the NCR-IS SAISO for ensuring the appropriate operational security posture is maintained for the NCR-IS Architecture and shall serve as the principal advisor to the aforementioned on all matters (technical and otherwise) involving the security of the system. The NCR-IS ISSO shall be responsible for monitoring and providing reports on IT security program matters to the NCR-IS SAISO for delivery to the NCR-IS CIO.

The **NCR-IS Architect** is responsible for the establishment and operation of electronic business processes to achieve the NCRIS strategy.

The **NCR-IS Operations Manager** is responsible for the operations and maintenance of telecommunications infrastructure, platforms, applications, and data services to ensure compliance with the technical and performance requirements outlined in the Service Level Agreement and Interconnection Agreement, the NCR-IS OM also performs critical infrastructure protection procedures in the event of a man made or natural disaster.

In addition, the NCR-IS Operations Manager provides technical facilities and support services to owners and users of information. The NCR-IS Operations Manager assists in the selection of cost effective controls to be used to protect information resources and is charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

The **NCR-IS Custodian** shall have the following generic responsibilities.

The Custodian is the intermediary organization or role involved in handling the jurisdictional or NCR-IS data (as it applies) as part of an information exchange/transaction. The Custodian can be an organization or a role in a particular organization.

The Custodian is responsible for complying with applicable federal, state, and local legislation and mandates, and policies as it applies to the data and security of the information exchange.

The **NCR-IS Data Steward** is responsible for the stewardship of data that is owned by NCR-IS. The generic responsibilities of a Data Steward are defined below.

The Data Steward provides advisement to the CIO on matters relative to ontologies, taxonomies and data architecture. The Data Steward ensures compliance with identified functional data requirements and is responsible for instituting critical infrastructure protection services to ensure the continued availability of information resources.

The Data Steward will also identify, provision, and maintain quality control of the data and metadata. The Data Steward will enforce the applicable standards and procedures in the



NCR Interoperability Services (NCR-IS)

Information Management Policy

organization; enforce naming standards and procedures; ensure proper use and data/metadata update procedure; and identify and provide the business rules for the data provided.

The **NCR-IS Administrator** (database admin/system admin) shall perform maintenance routines on data repositories to ensure optimum performance in operation, troubleshoot anomalies and irregularities discovered during operations of the information service, and archive and preserve data upon conclusion of the data lifecycle.

The NCR-IS Administrators are responsible for certain aspects of system security, such as adding and deleting user accounts as authorized by the NCR-IS ISO. The NCR-IS System Administrator may also assist in the identification of resources needed to effectively implement technical security controls. The System Administrator may also develop system administration and operational procedures and manuals as directed by the NCR-IS ISO.

The **NCR-IS Data Owner** is responsible for the ownership of data that is owned by the NCR-IS. This data can include audit records, login records, assignment of permissions to NCR-IS users, and other forms of information specific to NCR-IS systems. The generic responsibilities of a Data Owner are defined below.

The data owner is the primary owner of the data and all authority of the data rests with the data owner. The Data Owner is responsible to update the data as required, and is responsible for the creation, collection dissemination and maintenance of qualified, accurate, and timely data content; ensuring the cleanliness of data prior to submission to the NCR-IS; and provides timely notification to subscribers when the integrity of information is in question.

The **NCR-IS User** is any individual or automated application or process that is authorized access to the resource by the NCR-IS ISO, in accordance with the procedures and rules associated with the NCR-IS. All NCR-IS Users have the responsibility to comply with law, regulation, policy, standards and procedural controls in order to protect Information resources and authorized use of data within their custody. NCR-IS Users of data may be further decomposed to establish a role-based access structure in order to provide more granular access to applications and/or data.



Appendix B3: Glossary of Roles - NCR-IS Partner Roles

The following terms and descriptions represent roles and responsibilities applicable to NCR-IS Partners such as NCR jurisdictional personnel, NCR-IS Partner systems and services.

The **NCR-IS Partner Data Owner** is responsible for the ownership of data that is owned by the NCR-IS Partner. The generic responsibilities of a Data Owner are defined below.

The data owner is the primary owner of the data and all authority of the data rests with the data owner. The Data Owner is responsible to update the data as required, and is responsible for the creation, collection dissemination and maintenance of qualified, accurate, and timely data content; ensuring the cleanliness of data prior to submission to the NCR-IS; and provides timely notification to subscribers when the integrity of information is in question

The **NCR-IS Partner Data Steward** is responsible for the stewardship of data that is owned by NCR-IS. The generic responsibilities of a Data Steward are defined below.

The Data Steward provides advisement to the CIO on matters relative to ontologies, taxonomies and data architecture. The Data Steward ensures compliance with identified functional data requirements and is responsible for instituting critical infrastructure protection services to ensure the continued availability of information resources.

The Data Steward will also identify, provision, and maintain quality control of the data and metadata. The Data Steward will enforce the applicable standards and procedures in the organization; enforce naming standards and procedures; ensure proper use and data/metadata update procedure; and identify and provide the business rules for the data provided.

The **NCR-IS Custodian Partner** shall have the following generic responsibilities.

The Custodian Partner is the intermediary organization/role involved in handling the jurisdictional data as part of an information exchange/transaction. The Custodian Partner can be an organization or a role in a particular organization.

The **NCR-IS Consuming Partner** is the NCR-IS Partner organization which obtains information from the NCR-IS DEH.

The **NCR-IS Contributing Partner** is the NCR-IS Partner organization which provides information to the NCR-IS DEH.

The **NCR-IS Partner** is the organization representing a jurisdiction or system which will share information within the NCR-IS Architecture through a data exchange. The NCR-IS Partner shall serve as the designated owner of the information provided from their system or jurisdiction and will maintain responsibility for the ownership and integrity of the data they provide.

The **NCR-IS Partner Representative** is a designated representative who acts on behalf of the NCR-IS Partner with full authority of the NCR-IS Partner.

The **NCR-IS Partner User** is any individual or automated application or process that is authorized access to the resource by the NCR-IS ISO, in accordance with the procedures and rules of the corresponding NCR-IS Partner Data Owner. All NCR-IS Partner Users have the responsibility to comply with applicable laws, regulations, policies, standards and procedural controls in order to protect information resources and authorized use of data to which they have



NCR Interoperability Services (NCR-IS)

Information Management Policy

been authorized access. NCR-IS Partner Users of data may be further decomposed to establish a role-based access structure for more granular control of access to applications and/or data.

For Example: An NCR-IS Partner User may be a NCR jurisdiction employed dispatcher who accesses the NCR-IS Service to obtain data for operational purposes in order to know what fire trucks and other related equipment are available from the nearest jurisdictions.



NCR Interoperability Services (NCR-IS)

Information Management Policy

Appendix B4: Glossary of Roles - Services and Related Support Roles

The NCRIP DEH Project Team currently has the ability to draw upon a pool of skills sets consisting of an Enterprise Architects, Network Security Engineers, Interface Architects, Information Architects, Business/Technical Analysts and Software Engineers. The INETS and RWBN Team skills pool consists of similar engineers and architects who are capable of designing and deploying the networks. An assumption is made that the existing NCRIP project teams (DEH, INETS, RWBN) will receive sufficient FY05 and FY06 grant funding to remain intact and provide the services they have been providing through the Interim Maintenance and Operations Test period from March 2007 through July 2007. Additional skills sets required over and above those existing project teams to maintain the NCR-IS during the Interim Maintenance and Operations period are shown in the table on the following page.



NCR Interoperability Services (NCR-IS)

Information Management Policy

		Bs. /Tech Analyst	Software Engineer	Interface Architect	Information Architect	Network Engineer	Security Analyst	Technical Support Analyst & Specialists	Security Admin.	Web Site Admin	System Admin	Network Admin	DB Admin	Store/Cap/Per. Analyst	Telecomm Ops Technician	Operations Mgr / Analyst	CMDDB Admin. Service Desk Team	Training Coordinator
Analyze, Plan, Design, Build	Analyze INF Requirements	<p style="text-align: center;">Support to be provided By NCRIP Project teams Through July 2007</p>																
	Analyze A & E Requirements																	
	INF Planning																	
	A & E Planning																	
	INF Design																	
	A & E Design																	
	Build INF																	
	Build A & E's																	
Deploy & Operate *	Deploy INF	<p style="text-align: center;">Out-Sourcing Required for Interim M & O Period March – July 2007</p>																
	Deploy A & E's																	
	Operate INF																	
	Operate A & E's																	
Sec Mgt	Security Management																	
IT Service Mgt**	Optimize INF																	
	Optimize A & E's																	
	IT Service Support and Delivery																	

*Deploy and Operate includes Server Mgt, System and Storage Admin, Application Admin & Network Admin & Monitoring

** IT Service Management incorporates all ITIL Support and Delivery Processes

** IT Service Management incorporates all ITIL Support and Delivery Processes

INF = Infrastructure

A & E = Application and Exchanges

Figure 1. Matrix of Services and Related Support Roles



Appendix C: References

The following references describe in more detail the concepts in this report.

1. NCR Data Exchange Hub Architectural Recommendation, June 2006.
2. NCR Data Exchange Hub Data Sharing and Security Strategy, June 2006.
3. *NCR DEH Technical Requirements 2006_6_01 FINAL* for distribution, June 2006.
4. *NCR DEH Technology Guidelines 2006_04_24_FINAL* for distribution, June 2006.
5. NCR-IS Security Policy Document Version 1.
6. NCR-IS Service Management Framework Version 1.
7. NCR-IS Service Management Service Catalog Version 1.
8. *NCR-IS IEPD Catalog*, <http://www.ncrnet.us/deh/IEPD/NCRIPDEHClearingHouse.html>
9. Anne Marie Smith, *BEST PRACTICES IN METADATA MANAGEMENT – AN OVERVIEW*, Alabama Yankee Systems, TDAN.com, April 2006, Available at <http://www.tdan.com/i036ht02.htm>.
10. Federal Enterprise Architecture Data Reference Model (DRM) Version 2.0, November 17 2005, <http://www.whitehouse.gov/omb/egov/a-5-drm.html>.
11. Federal Enterprise Architecture DRM Data Management Strategy DRAFT, February 2004.
12. Michael J. Belcher, *What Metadata is and Why You Should Care*, 2H05 Through 1H06, July 2, 2005, Gartner Inc., Publication Number G00127890
13. Pipino et al., *Data Quality Assessment*, Available at <http://web.mit.edu/tdqm/www/tdqmpub/PipinoLeeWangCACMApr02.pdf>.