



# **National Capital Region Interoperability Services (NCR-IS)**

## **Information Technology (IT) Service Management (ITSM) 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)

## IT Service Management (ITSM) Policy

### Executive Summary

NCR-IS Partners require that the NCR-IS Information Technology (IT) Infrastructure reliably deliver the appropriate IT services when they are needed. The NCR-IS is currently designing an Information Technology Infrastructure Library (ITIL) compliant IT Service Management (ITSM) capability to support NCR-IS Partners. The ITSM function will manage the comprehensive IT services required by the NCR-IS business partners. The ultimate goal is to provide a single IT Service Desk (i.e. single number to call) for all issues related to maintaining and supporting regional interoperable communications.

#### ITIL-Based IT Service Management

ITIL provides a consistent and coherent set of best practices for IT Service Management processes. These ITSM processes are intended to be implemented to support, not dictate, the business processes of an organization. ITIL is based on the collective experience of commercial and governmental agencies worldwide and is fast becoming the de facto standard for ITSM. ITIL is the most widely accepted approach to ITSM in the world and it will provide a sound foundation for designing and building ITSM capabilities for the NCR-IS IT Infrastructure.

ITIL contains an integrated set of well-documented processes including: Service Desk, Incident Management, Problem Management, Change Management, Release Management, Configuration Management, Service Level Management, Availability Management, Capacity Management, Financial Management for IT services and IT Service Continuity Management. These processes are used to manage, deliver, and measure the provisioning of services. Figure 1 below depicts the overall ITIL framework and the relationship between ITSM processes and services.

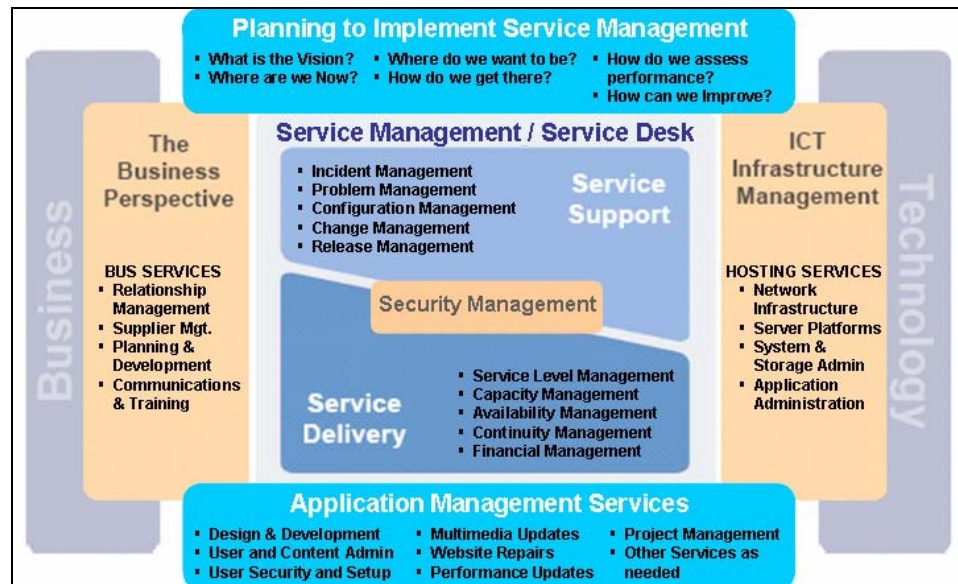


Figure 1. ITIL Framework



## **NCR Interoperability Services (NCR-IS)**

### **IT Service Management (ITSM) Policy**

---

The policy for the NCR-IS IT Infrastructure is to use this framework as a guideline for formulating our ITSM strategy for the region and for supporting the IT Services Catalog to be available to NCR-IS Partners using the NCR-IS IT Infrastructure for secure wired or wireless networking and for facilitating applications and exchanges.

### **ITSM Planning Approach**

Implementing ITSM processes and capabilities takes careful planning and a recognition that comprehensive ITSM cannot be built at once. The NCR-IS is identifying the short-term and long-term ITSM processes and services. Much of the effort is currently focused on developing an NCR-IS IT Customer Oriented Service Catalog which describes the professional and IT services that will be offered. Initially the scope of the NCR-IS Service catalog will pertain to providing support for the initial Exchanges and related NCR-IS initiated networking infrastructures which include:

- NCR-IS Data Exchange Hub
- NCRnet
- RWBN (Regional Wireless Broadband Network)

The following IT support process and service domains and their relationships form the foundation of the NCR-IS ITIL-based ITSM framework:

- IT Service Support Processes including:
  - Incident Management
  - Problem Management
  - Configuration Management
  - Change Management
  - Release Management
- IT Service Delivery Processes
  - Service Level Management
  - Capacity Management
  - Availability Management
  - Continuity Management
  - Financial Management
- IT Customer-Oriented Service Catalog
  - ICT Infrastructure Management Services
  - Application Management Services
  - Security Management Services
  - Business Services



## **NCR Interoperability Services (NCR-IS)**

---

### IT Service Management (ITSM) Policy

Each of the domains above and their interrelationships are described in the ITSM Policy.

While definition of the NCR-IS ITSM Policy and the NCR-IS Operational Plan will be an iterative and on-going process as the enterprise matures, it is the purpose of this document to provide the foundation for that dialog in order to provide guidance on the processes and services necessary to provide interim maintenance and support for the NCR-IS DEH, NCRnet and RWBN beginning September 2007.



# NCR Interoperability Services (NCR-IS)

## IT Service Management (ITSM) Policy

### Table of Contents

<b>1</b>	<b>OVERVIEW.....</b>	<b>1</b>
<b>2</b>	<b>PURPOSE.....</b>	<b>1</b>
<b>3</b>	<b>OBJECTIVES.....</b>	<b>2</b>
<b>4</b>	<b>SCOPE.....</b>	<b>3</b>
<b>5</b>	<b>THE NCR-IS ITSM POLICY .....</b>	<b>4</b>
5.1	IT SERVICE MANAGEMENT (ITSM) PROCESSES .....	6
5.1.1	IT Service Support Processes .....	6
5.1.1.1	Incident Management.....	6
5.1.1.2	Problem Management .....	6
5.1.1.3	Configuration Management.....	6
5.1.1.4	Change Management.....	6
5.1.1.5	Release Management .....	7
5.1.2	IT Service Delivery Processes .....	7
5.1.2.1	Service Level Management.....	7
5.1.2.2	Capacity Management.....	7
5.1.2.3	Availability Management.....	7
5.1.2.4	Continuity Management.....	8
5.1.2.5	Financial Management.....	8
5.2	IT CUSTOMER-ORIENTED SERVICE CATALOG .....	8
5.2.1	ICT Infrastructure Management Services.....	9
5.2.2	Application / Exchange Management Services.....	9
5.2.3	Security Management Services.....	9
5.2.4	Business Services.....	10
	<b>APPENDIX A: GLOSSARY OF TERMS, ROLES AND POSITIONS .....</b>	<b>12</b>
	APPENDIX A1: GLOSSARY OF TERMS.....	12
	APPENDIX A2: GLOSSARY OF ROLES - NCR-IS CENTRAL ROLES .....	18
	APPENDIX A3: GLOSSARY OF ROLES - NCR-IS PARTNER ROLES .....	21
	APPENDIX A4: GLOSSARY OF ROLES - SERVICES AND RELATED SUPPORT ROLES .....	23

### List of Figures

Figure 1.	ITIL Framework .....	ii
Figure 2.	NCR-IS SOA Governance Structure .....	1
Figure 3.	NCR-IS Service Desk Process.....	3
Figure 4.	The ITIL Service Management Framework Relationships.....	5
Figure 5.	Matrix of Services and Related Support Roles .....	24



# NCR Interoperability Services (NCR-IS)

## IT Service Management (ITSM) Policy

### 1 Overview

The NCR-IS Architecture is designed using a Services Oriented Architecture, that is currently comprised of three major components, the Data Exchange Hub (DEH), NCRnet and Regional Wireless Broadband Network (RWBN). This architecture will utilize the IT Infrastructure Library framework as a basis for defining and implementing its Service Management Strategy for the NCR-IS. Maintenance and operational governance will control the production of artifacts and monitor compliance with standards. This will help stakeholders measure whether projects requesting support from the NCR-IS infrastructure are aligned with regional standards and meet the needs of the business users. For more information, see the figure below.

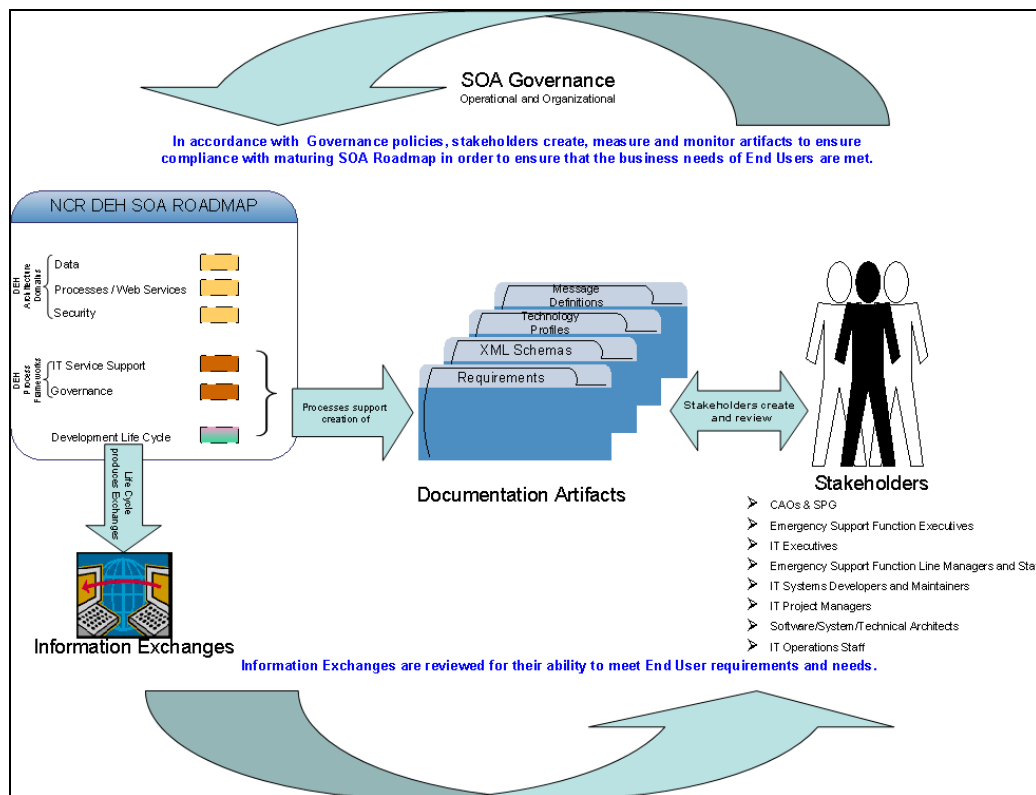


Figure 2. NCR-IS SOA Governance Structure

### 2 Purpose

The purpose of this document is to set forth the policy for establishing the NCR-IS IT Service Management (ITSM) function. This document is intended to provide policies for the processes and services that will be provided by the NCR-IS ITSM organization.



## NCR Interoperability Services (NCR-IS)

### IT Service Management (ITSM) Policy

---

## 3 Objectives

The main objective of the NCR-IS ITSM Policy is to document policies governing the establishment of the NCR-IS IT support processes and services. The policy will reference the initial services are processes that will be delivered and supported by the NCR-IS ITSM organization. The policy can also provide a baseline for a Service Level Agreements (SLA), or even potentially replace SLAs in some cases. It will provide a basis from which to document procedures and processes in the NCR-IS. In order to be effective the ITSM Policy must be understood and embraced by the customers and jurisdictions wishing to use the NCR-IS.

The NCR-IS will provide leading, best practices IT service support by building upon the industry standard Information Technology Infrastructure Library (ITIL). Being a framework, ITIL describes the contours of organizing *Service Management*. The models show the goals, general activities, inputs and outputs of the various processes, which can be incorporated within organizations. ITIL does not cast in stone every action required on a day-to-day basis because that is something which differs from organization to organization. Instead it focuses on best practice that can be utilized in different ways according to need. The scope of ITIL and its individual elements is shown in Figure 1 in the Executive Summary. By emphasizing the relationships between the processes, any lack of communication and co-operation between various IS functions can be minimized or eliminated. ITIL provides a proven method for planning common processes, roles and activities with appropriate reference to each other and how the communication lines should function between them.

Support for regional IT solutions will require a coordinated effort between existing Service Desks of the NCR-IS Partners within the region and the NCR-IS. Considerable planning and coordination will need to occur. IT and ESF Staff from NCR-IS Partners will be the primary users of the NCR-IS. At a conceptual level, it is envisioned that support will be a multi-tiered process. Most calls will originate within the Service Desks of the NCR-IS Partners and then be escalated as needed to the NCR-IS Service Desk. This document is an attempt to define the processes and services that would be provided by the NCR-IS at the Tier 2 and Tier 3 levels highlighted in the NCR-IS IT Service Management Process diagram below. The ultimate goal of the NCR-IS is to provide a single IT Service Desk (i.e. single number to call) for all issues related to maintaining and supporting regional Interoperable Communications.



# NCR Interoperability Services (NCR-IS)

## IT Service Management (ITSM) Policy

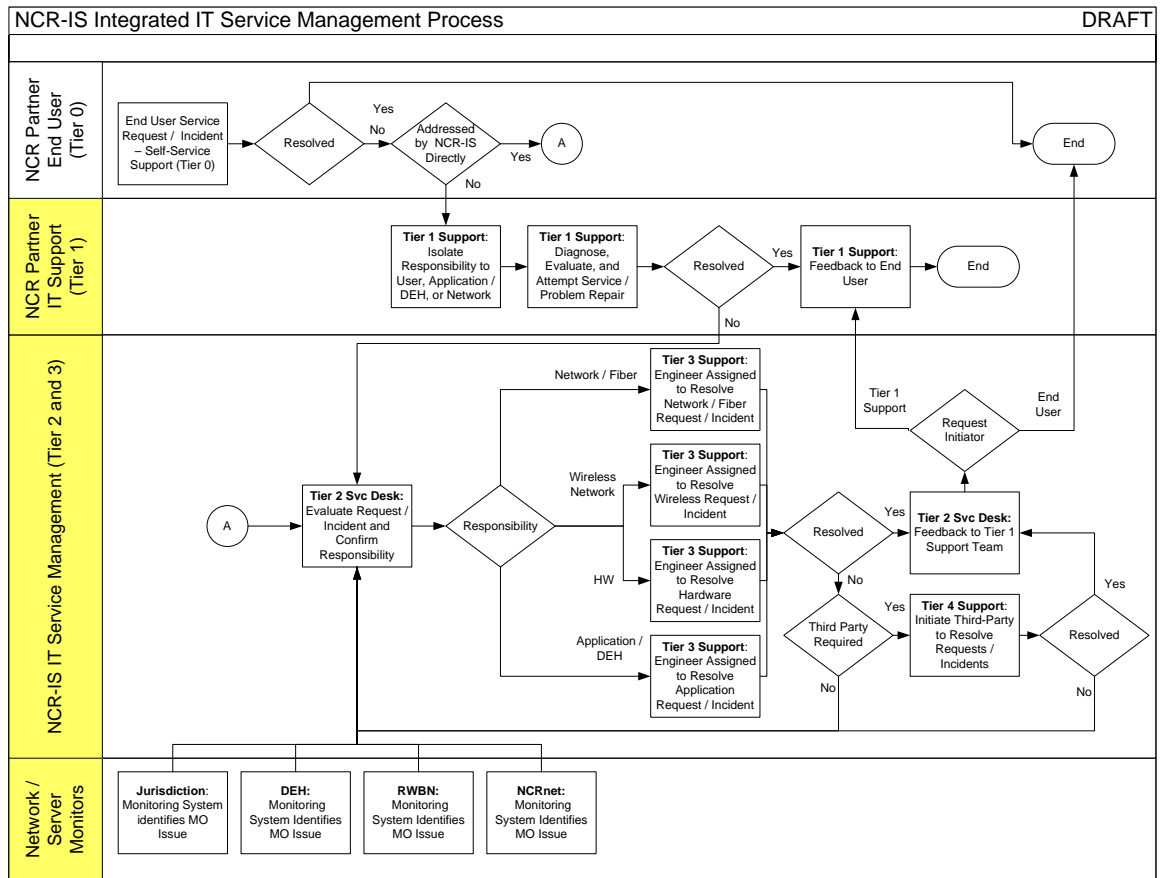


Figure 3. NCR-IS Service Desk Process

## 4 Scope

Initially the scope of the NCR-IS ITSM Policy will be to provide support for the initial Exchanges and related NCR-IS initiated networking infrastructures which include:

- NCR-IS Data Exchange Hub - The purpose of the DEH is to enable the secure, efficient exchange of information (text, voice, video and multimedia) between Emergency Support Functions (ESFs) in region.
- NCRnet - The primary purpose of the NCRnet is to provide a reliable and available, high speed, fiber optic network to allow emergency responders, police, fire, and other supporting personnel to communicate in the event of natural or man-made emergencies or disasters. It is independently operated and maintained by the NCR jurisdictions and its designees.
- RWBN - The primary purpose of the RWBN is to provide a mobile, high speed, and available wireless voice and data infrastructure to allow emergency personnel to communicate in the event of natural or man-made emergencies or disasters. It is independently operated and maintained by the NCR jurisdictions and its designees.



## **NCR Interoperability Services (NCR-IS)**

### **IT Service Management (ITSM) Policy**

---

The following IT Service Management domains and the relationships between them are discussed in this policy:

- IT Service Support Processes including:
  - Incident Management
  - Problem Management
  - Configuration Management
  - Change Management
  - Release Management
- IT Service Delivery Processes
  - Service Level Management
  - Capacity Management
  - Availability Management
  - Continuity Management
  - Financial Management
- IT Customer-Oriented Service Catalog
  - ICT Infrastructure Management Services
  - Application Management Services
  - Security Management Services
  - Business Services

## **5 The NCR-IS ITSM Policy**

This NCR-IS ITSM Policy will describe in detail the ITSM processes (including Service Support and Service Delivery); and ICT Infrastructure Management, Application Management, Security Management, and Business services envisioned for the NCR-IS. The diagram shown below identifies the relationship between the ITSM processes and services.



# NCR Interoperability Services (NCR-IS)

## IT Service Management (ITSM) Policy

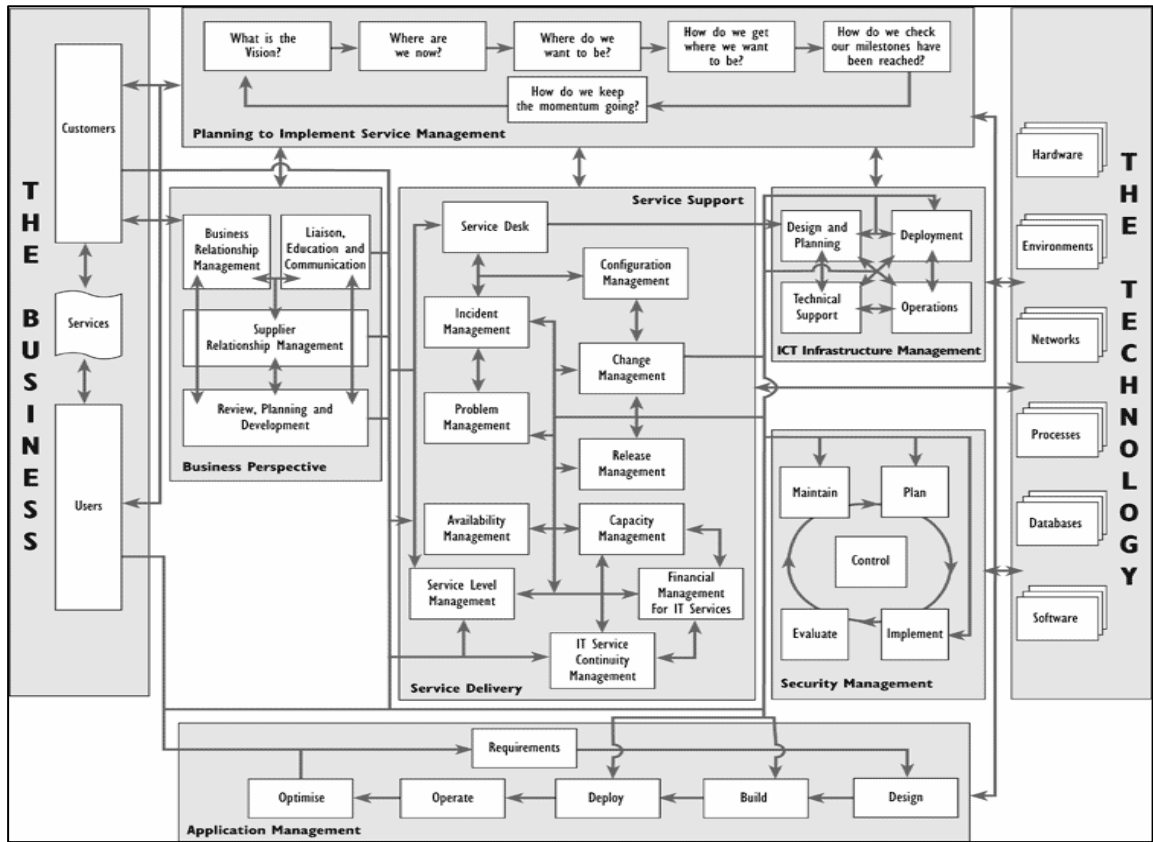


Figure 4. The ITIL Service Management Framework Relationships



## NCR Interoperability Services (NCR-IS)

### IT Service Management (ITSM) Policy

## 5.1 IT Service Management (ITSM) Processes

Processes associated with IT Service Management specifically IT Service Support and IT Service Delivery processes are defined in the table below. Initially NCR-IS IT Service Management (ITSM) will focus on Incident Management, Configuration Management, Change Management, Service Level Management and Release Management. Future phases will incorporate the remaining IT Service Support and Delivery Processes.

### 5.1.1 IT Service Support Processes

5.1.1.1 Incident Management	
<b>Description:</b>	The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.
5.1.1.2 Problem Management	
<b>Description:</b>	Problem Management minimizes the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure, and prevents recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation. Problem Management also needs to liaise closely with the availability management process to identify these trends and instigate remedial action.
5.1.1.3 Configuration Management	
<b>Description:</b>	Configuration Management identifies relationships between an item that is to be changed and any other components of the infrastructure, thus allowing the owners of these components to be involved in the impact assessment process.
5.1.1.4 Change Management	
<b>Description:</b>	Change Management process ensures that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization. The Change Management process depends on the accuracy of the configuration data to ensure the full impact of making changes is known. There is therefore a very close relationship between Configuration Management,



## NCR Interoperability Services (NCR-IS)

### IT Service Management (ITSM) Policy

	Release Management and Change Management.
<b>5.1.1.5 Release Management</b>	
<b>Description:</b>	Changes may often result in the need for new hardware, new versions of software, and/or new documentation, created in-house or bought in, to be controlled and distributed, as part of a new 'packaged Release'. Release Management if for ensuring secure, managed rollout should be closely integrated with those for Change Management and Configuration Management. Release procedures may also be an integral part of Incident Management and Problem Management, as well as being closely linked to the CMDB in order to maintain up-to-date records.

## 5.1.2 IT Service Delivery Processes

<b>5.1.2.1 Service Level Management</b>	
<b>Description:</b>	The Service Level Management (SLM) process is responsible for ensuring Service Level Agreements (SLAs) and other contracts are met, and for ensuring that any adverse impact on service quality is kept to a minimum. The process involves assessing the impact of Changes upon service quality and SLAs, both when Changes are proposed and after they have been implemented. Some of the most important targets set in the SLAs will relate to service availability and thus require Incident resolution within agreed periods. SLM is the hinge for Service Support and Service Delivery. It cannot function in isolation as it relies on the existence and effective and efficient working of other processes. An SLA without underpinning support processes is useless, as there is no basis for agreeing to its content.
<b>5.1.2.2 Capacity Management</b>	
<b>Description:</b>	Capacity Management is responsible for ensuring adequate capacity is available at all times to meet the requirements of the business. It is directly related to the business requirements and is not simply about the performance of the system's components, individually or collectively. Capacity Management is involved in Incident resolution and Problem identification for those difficulties relating to capacity issues.
<b>5.1.2.3 Availability Management</b>	



## NCR Interoperability Services (NCR-IS)

### IT Service Management (ITSM) Policy

<p><b>Description:</b></p>	<p>Availability Management is concerned with the design, implementation, measurement and management of IT services to ensure the stated business requirements for availability are consistently met. Availability Management requires an understanding of the reasons why IT service failures occur and the time taken to resume service. Incident Management and Problem Management provide a key input to ensure the appropriate corrective actions.</p>
<p><b>5.1.2.4 Continuity Management</b></p>	
<p><b>Description:</b></p>	<p>IT Service Continuity must be derived so as to be flexible enough to support all the contingency options anticipated by the business in their Business Continuity Plans. And where IT is not the only service provider affected, it is necessary to consider how IS support for the other internal service providers may, in turn, be affected. When it comes to deciding on continuity strategies, the business may well take a different risk-based perspective than that adopted or anticipated by IT.</p>
<p><b>5.1.2.5 Financial Management</b></p>	
<p><b>Description:</b></p>	<p>Financial Management is responsible for accounting for the costs (costing) and return on IT service investments (IT portfolio management), and for any aspects of recovering costs from the Customers (charging). It requires good interfaces with Capacity Management, Configuration Management (asset data) and Service Level Management to identify the true costs of service. Financial Management is likely to work closely with Business Relationship Management and the IT organization during the negotiations of the IT organization's budgets and individual Customer's IT spending.</p>

## 5.2 IT Customer-Oriented Service Catalog

The IT Customer-Oriented Service Catalog describes the IT services that will be provided by the NCR-IS to NCR-IS Partner jurisdiction / agency users. Initially, the NCR-IS will be focused on providing the core, necessary services to operate the NCR-IS infrastructure. As the NCR-IS matures, it will offer additional performance and professional services as required by its customers.

IT services can be categorized in the following areas:

- ICT Infrastructure Management Services
- Application / Exchange Management Services
- Security Management Services



## **NCR Interoperability Services (NCR-IS)**

### **IT Service Management (ITSM) Policy**

---

- Business Services

The following descriptions offer an overview of the different IT service types. The NCR-IS Customer-Oriented Service Catalog will contain additional details for each IT service provided by the NCR-IS.

#### **5.2.1 ICT Infrastructure Management Services**

Information and Communications Technology (ICT) services will support the design / planning, deployment, operations, and technical support of the entire NCR-IS infrastructure. The NCR-IS infrastructure may include application and database servers, distributed systems, networks and network components, desktop workstations, and mobile devices. The infrastructure will evolve as the NCR-IS matures and changes to meet increasing operational needs.

Initially, NCRIP project teams will support and deliver the design / planning and deployment services related to any ICT infrastructure component. The NCR-IS will support deployment into the NCR-IS environment and will primarily provide operations and technical support services once the infrastructure is deployed. Examples of ICT Infrastructure Management Services include:

- Account Management Services
- Connectivity Services
- Data Center Services
- Network Services.

The NCR-IS Customer-Oriented Service Catalog will maintain an on-going record of the specific IT infrastructure management services to be provided by the NCR-IS.

#### **5.2.2 Application / Exchange Management Services**

Application / Exchange Management services address the complex subject of managing applications and exchanges throughout their lifecycle. Application / Exchange services include business requirements, design, build, deployment, operations, optimization, and data management services. Initially, NCRIP project teams will be responsible for requirements, design, build, and deployment services related to applications and exchanges. The NCR-IS will work in conjunction with the NCRIP teams during deployment and will then offer ongoing operational services.

The NCR-IS Service Catalog will maintain a record of the specific application / exchange services to be provided by the NCR-IS over time.

#### **5.2.3 Security Management Services**

The goal of the NCR-IS Security Management service is two-fold:



## NCR Interoperability Services (NCR-IS)

### IT Service Management (ITSM) Policy

---

- Provide services to meet the *external* security requirements. These result from the security requirements in the various [SLAs](#). These external requirements for security also stem from contracts, legislation and any imposed security policies of NCR-IS Partners.
- Provide services to meet the *internal* security requirements. This is required to assure the IT service provider's own continuity. It is also necessary to simplify the [Service Level Management](#) for information security. After all, managing a large number of different SLAs is much more complex than managing a small number. Therefore, for instance, a certain basic level of security (the so-called standard security *baseline*) needs to be established.

The NCR-IS Security Management services are governed by the NCR-IS Security Policy. That policy sets forth the approved and disapproved uses of NCR Interoperability Services. Within the ITIL framework, security information is contained in the Service Level Agreements established for each service offered by the NCR-IS. The NCR-IS acknowledges that security processes must support the business needs. Furthermore, to use what is already available, standard ITIL processes have integrated Security Management principles wherever possible. The integrated security tasks within each ITIL process should take care of the security aspects in their specific area, but the point of control of these tasks is centralized by the security management process. Security management services ensure the confidentiality, integrity, and availability of information and information systems. Privacy, anonymity, and verifiability can be extrapolated from these information security pillars. Security management seeks to apply measures, or security controls, that are preventive, reductive, detective, repressive, and corrective in nature.

Evaluation processes are also employed to examine and report on security incidents which may or may not have impacted business services and compliance with the corresponding SLAs. Because ITIL contains management processes for information technology, the management of personnel and physical entities are not specifically addressed. Measures and operations related to the management of people and facilities can be different from those which manage information technology. ITIL is a framework for managing information technology, not facilities or people. Measures and operations for personnel and facilities can be defined during the evolution of the NCR-IS.

#### 5.2.4 Business Services

The NCR-IS will need to interact with NCR-IS Partners on a regular basis to identify business needs and opportunities and undertake appropriate capacity planning in anticipation of future applications and exchanges. Once a specific business need is identified, the NCR-IS will need to assist business users in planning and preparing documentation for review and consideration by the MWCOG ARC and CIOs who will assess conformance of the proposed solution with the NCR-IS architecture. Additionally, NCR-IS, following in the footsteps of the NCRIP DEH Project, will need to provide assistance in educating and training NCR-IS Partner staff on emerging technologies and solutions that will be deployed within the NCR-IS Infrastructure.

Initially, the NCR-IS will provide the following types of business services:

- Knowledge Management Services



## **NCR Interoperability Services (NCR-IS)**

---

### IT Service Management (ITSM) Policy

- Project Management Services

The NCR-IS Service Catalog will maintain a record of the specific business services to be provided by the NCR-IS and it will be updated over time as services evolve keep up with customer needs.



## Appendix A: Glossary of Terms, Roles and Positions

### Appendix A1: 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)

### IT Service Management (ITSM) 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) [10]

**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<sup>1</sup>.

Note, that 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 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

---

<sup>1</sup> 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)**

### **IT Service Management (ITSM) Policy**

---

**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](http://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).

**Homeland Security Information Network (HSIN)** HSIN Critical Infrastructure Pilot is an unclassified network and governance program providing a nation-wide platform that enables sharing of essential homeland security information with the proper stakeholders. This information sharing is accomplished both horizontally across the government and vertically



## **NCR Interoperability Services (NCR-IS)**

### **IT Service Management (ITSM) Policy**

---

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** is 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.

**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.



## **NCR Interoperability Services (NCR-IS)**

### IT Service Management (ITSM) Policy

---

**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 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, 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.



## **NCR Interoperability Services (NCR-IS)**

### **IT Service Management (ITSM) Policy**

---

**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 the delivery of one or more services which enable a business process.

**Service Level Agreement (SLA)** is 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 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)**

### IT Service Management (ITSM) Policy

---

## **Appendix A2: 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)**

### IT Service Management (ITSM) 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 ontology, 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)**

### **IT Service Management (ITSM) 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 A3: 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 ontology, 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)**

---

### IT Service Management (ITSM) 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.

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)**

IT Service Management (ITSM) Policy

---

### **Appendix A4: 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)

## IT Service Management (ITSM) 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	CMDB Admin.	Service Desk Team	Training Coordinator
Analyze, Plan, Design, Build	Analyze INF Requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Analyze A & E Requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	INF Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	A & E Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	INF Design	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	A & E Design	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Build INF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Build A & E's	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Deploy & Operate *	Deploy INF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	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 5. Matrix of Services and Related Support Roles