



National Capital Region Interoperability Services (NCR-IS)

Security Policy v1.0 for distribution

[Applies to the Protection of Data up to the Sensitive but Unclassified (SBU) Level]

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)

Security Policy

Executive Summary

The National Capital Region Interoperability Services (NCR-IS) shall be responsible for transporting data, in the form of voice, text, images, and video, between NCR jurisdictions primarily to support the prevention, protection, response, and recovery efforts prior to or during major natural or man-made events. This information can range from network outage notifications, electronic mail, or personnel skill set data, to the availability of shelters within a jurisdiction, the location and availability of emergency equipment, or teleconference situational reports during a major event affecting one or more NCR jurisdictions.

The NCR-IS shall fulfill these capabilities using electronic data exchanges and a combination of wireless and wire line networking technologies. The information passed over these mechanisms must be protected from unauthorized use, modification and inspection. The NCR-IS Security Policy, along with supporting processes and procedures, sets forth policy for the secure establishment and operation of the (NCR-IS). The intent of the controls recognized in this policy is to protect the confidentiality, integrity, and availability of the NCR-IS and the information contained or exchanged by the NCR-IS with NCR-IS Partners.

The structure of the security policy follows publicly-available documentation from the National Institute of Standards and Technology and existing security policies of NCR-member jurisdictions. The policy uses the established NCR-IS Roles and Responsibilities to define those necessary functions, to be assigned to an individual or group of individuals, which need to be performed for the NCR-IS to be managed, operated and maintained.

Ultimately, this policy shall create a foundation for the development of assessment methods and procedures for determining the security control effectiveness.



Table of Contents

1	PURPOSE	2
2	OBJECTIVES	2
3	SCOPE	2
4	ROLES AND RESPONSIBILITIES	2
5	MANAGEMENT SECURITY POLICY	2
5.1	RISK ASSESSMENT	2
5.1.1	<i>Risk Assessment Policy and Procedures</i>	2
5.1.2	<i>Security Categorization</i>	2
5.1.3	<i>Risk Assessment</i>	2
5.1.4	<i>Vulnerability Assessment</i>	2
5.2	PLANNING	2
5.2.1	<i>Security Planning Policy and Procedures</i>	2
5.2.2	<i>System Security Plan</i>	2
5.2.3	<i>Rules of Behavior</i>	2
5.3	SYSTEM & SERVICES ACQUISITION	2
5.3.1	<i>System and Services Acquisition Policy and procedures</i>	2
5.3.2	<i>Allocation of Resources</i>	2
5.3.3	<i>Life Cycle Support</i>	2
5.3.4	<i>Acquisitions</i>	2
5.3.5	<i>Documentation</i>	2
5.3.6	<i>Software Usage Restrictions</i>	2
5.3.7	<i>User Installed Software</i>	2
5.3.8	<i>Security Design Principles</i>	2
5.3.9	<i>Outsourced Services</i>	2
6	OPERATIONAL SECURITY POLICY	2
6.1	PERSONNEL SECURITY	2
6.1.1	<i>Personnel Security Policy and Procedures</i>	2
6.1.2	<i>Position Categorization</i>	2
6.1.3	<i>Personnel Screening</i>	2
6.1.4	<i>Personnel Termination</i>	2
6.1.5	<i>Personnel Transfer</i>	2
6.1.6	<i>Access Agreements</i>	2
6.1.7	<i>Third-Party Personnel Security</i>	2
6.1.8	<i>Personnel Sanctions</i>	2
6.2	PHYSICAL & ENVIRONMENTAL PROTECTION	2
6.2.1	<i>Physical and Environmental Protection Policy and Procedures</i>	2
6.2.2	<i>Physical Access Authorizations</i>	2
6.2.3	<i>Physical Access Control</i>	2
6.2.4	<i>Access Control for Display</i>	2
6.2.5	<i>Monitoring Physical Access</i>	2
6.2.6	<i>Visitor Control</i>	2
6.2.7	<i>Access Logs</i>	2
6.2.8	<i>Power Equipment and Power Cabling</i>	2
6.2.9	<i>Emergency Shutoff</i>	2
6.2.10	<i>Emergency Power</i>	2
6.2.11	<i>Fire Protection</i>	2



NCR Interoperability Services (NCR-IS)

Security Policy

6.2.12	<i>Temperature and Humidity Controls</i>	2
6.2.13	<i>Water Damage Protection</i>	2
6.2.14	<i>Delivery and Removal</i>	2
6.2.15	<i>Alternate Work Site</i>	2
6.3	CONTINGENCY PLANNING.....	2
6.3.1	<i>Contingency Planning Policy and Procedures</i>	2
6.3.2	<i>Contingency Plan</i>	2
6.3.3	<i>Contingency Training</i>	2
6.3.4	<i>Contingency Plan Testing</i>	2
6.3.5	<i>Alternate Storage Site</i>	2
6.3.6	<i>Alternate Processing Site</i>	2
6.3.7	<i>Telecommunications Service</i>	2
6.3.8	<i>NCR-IS Architecture Backup</i>	2
6.3.9	<i>NCR-IS Architecture Recovery and Reconstitution</i>	2
6.4	CONFIGURATION MANAGEMENT.....	2
6.4.1	<i>Configuration Management Policy and Procedures</i>	2
6.4.2	<i>Baseline Configuration</i>	2
6.4.3	<i>Configuration Change Control</i>	2
6.4.4	<i>Monitoring Configuration Changes</i>	2
6.4.5	<i>Access Restrictions for Change</i>	2
6.4.6	<i>Configuration Settings</i>	2
6.4.7	<i>Least Functionality</i>	2
6.5	MAINTENANCE.....	2
6.5.1	<i>System Maintenance Policy and Procedures</i>	2
6.5.2	<i>Periodic Maintenance</i>	2
6.5.3	<i>Maintenance Tools</i>	2
6.5.4	<i>Remote Maintenance</i>	2
6.5.5	<i>Maintenance Personnel</i>	2
6.5.6	<i>Timely Maintenance</i>	2
6.6	SYSTEM & INFORMATION INTEGRITY.....	2
6.6.1	<i>System and Information Integrity Policy and Procedures</i>	2
6.6.2	<i>Flaw Remediation</i>	2
6.6.3	<i>Malicious Code Protection</i>	2
6.6.4	<i>Intrusion Detection Tools and Techniques</i>	2
6.6.5	<i>Security Alerts and Advisories</i>	2
6.6.6	<i>Security Functionality Verification</i>	2
6.6.7	<i>Software and Information Integrity</i>	2
6.6.8	<i>Spam and Spyware Protection</i>	2
6.6.9	<i>Information Input Restrictions (accuracy, completeness, and validity)</i>	2
6.6.10	<i>Information Output Handling and Retention</i>	2
6.6.11	<i>Error Handling</i>	2
6.6.12	<i>Information Output Handling and Retention</i>	2
6.7	MEDIA PROTECTION.....	2
6.7.1	<i>Media Protection Policy and Procedures</i>	2
6.7.2	<i>Media Access</i>	2
6.7.3	<i>Media Labeling</i>	2
6.7.4	<i>Media Storage</i>	2
6.7.5	<i>Media Transport</i>	2
6.7.6	<i>Media Sanitization</i>	2
6.7.7	<i>Media Destruction and Disposal</i>	2
6.8	INCIDENT RESPONSE.....	2
6.8.1	<i>Incident Response Policy and Procedures</i>	2
6.8.2	<i>Incident Response Training</i>	2



NCR Interoperability Services (NCR-IS)

Security Policy

6.8.3	<i>Incident Response Testing</i>	2
6.8.4	<i>Incident Handling</i>	2
6.8.5	<i>Incident Monitoring</i>	2
6.8.6	<i>Incident Reporting</i>	2
6.8.7	<i>Incident Response Assistance</i>	2
6.9	SECURITY AWARENESS TRAINING	2
6.9.1	<i>Security Awareness and Training Policy and Procedures</i>	2
6.9.2	<i>Security Awareness</i>	2
6.9.3	<i>Security Training</i>	2
6.9.4	<i>Security Training Records</i>	2
7	TECHNICAL SECURITY POLICY	2
7.1	IDENTIFICATION & AUTHENTICATION	2
7.1.1	<i>Identification and Authentication Policy and Procedures</i>	2
7.1.2	<i>User Identification and Authentication</i>	2
7.1.3	<i>Device Identification and Authentication</i>	2
7.1.4	<i>Identifier Management</i>	2
7.1.5	<i>Authenticator Management</i>	2
7.1.6	<i>Authentication Feedback</i>	2
7.1.7	<i>Cryptographic Module Authentication</i>	2
7.2	ACCESS CONTROL	2
7.2.1	<i>Access Control Policy and Procedures</i>	2
7.2.2	<i>Account Management</i>	2
7.2.3	<i>Access Enforcement</i>	2
7.2.4	<i>Information Flow Enforcement</i>	2
7.2.5	<i>Separation of Duties</i>	2
7.2.6	<i>Least Privilege</i>	2
7.2.7	<i>Unsuccessful Login Attempts</i>	2
7.2.8	<i>System Use Notification</i>	2
7.2.9	<i>Concurrent Session Lock</i>	2
7.2.10	<i>Session Lock</i>	2
7.2.11	<i>Session Termination</i>	2
7.2.12	<i>Supervision and Review – Access Control</i>	2
7.2.13	<i>Permitted Actions without Identification and Authentication</i>	2
7.2.14	<i>Automated Marking</i>	2
7.2.15	<i>Remote Access</i>	2
7.2.16	<i>Wireless Access Restrictions</i>	2
7.2.17	<i>Access Control for Portable and Mobile Devices</i>	2
7.2.18	<i>Personally Owned NCR-IS Architectures</i>	2
7.3	AUDIT & ACCOUNTABILITY	2
7.3.1	<i>Audit and Accountability Policy and Procedures</i>	2
7.3.2	<i>Auditable Events</i>	2
7.3.3	<i>Content of Audit Records</i>	2
7.3.4	<i>Audit Storage Capacity</i>	2
7.3.5	<i>Audit Processing</i>	2
7.3.6	<i>Audit Monitoring, Analysis, and Reporting</i>	2
7.3.7	<i>Audit Reduction and Report Generation</i>	2
7.3.8	<i>Time Stamps</i>	2
7.3.9	<i>Protection of Audit Information</i>	2
7.3.10	<i>Audit Retention</i>	2
7.4	SYSTEM & COMMUNICATION PROTECTION	2
7.4.1	<i>System and Communications Protection Policy and Procedures</i>	2
7.4.2	<i>Application Partitioning</i>	2



NCR Interoperability Services (NCR-IS)

Security Policy

7.4.3	<i>Security Function Isolation</i>	2
7.4.4	<i>Information Remnants</i>	2
7.4.5	<i>Denial of Service</i>	2
7.4.6	<i>Resource Priority</i>	2
7.4.7	<i>Boundary Protection</i>	2
7.4.8	<i>Transmission Integrity</i>	2
7.4.9	<i>Transmission Confidentiality</i>	2
7.4.10	<i>Network Disconnect</i>	2
7.4.11	<i>Cryptographic Key Establishment and Management</i>	2
7.4.12	<i>Use of Validated Cryptography</i>	2
7.4.13	<i>Public Access Protections</i>	2
7.4.14	<i>Collaborative Computing</i>	2
7.4.15	<i>Public Key Infrastructure Certificates</i>	2
7.4.16	<i>Mobile Code</i>	2
7.4.17	<i>Voice Over Internet Protocol</i>	2
APPENDIX A: GLOSSARY OF TERMS, ROLES AND POSITIONS		2
APPENDIX A1: GLOSSARY OF TERMS		2
APPENDIX A2: GLOSSARY OF ROLES - NCR-IS CENTRAL ROLES.....		2
APPENDIX A3: GLOSSARY OF ROLES - NCR-IS PARTNER ROLES		2
APPENDIX A4: GLOSSARY OF ROLES - SERVICES AND RELATED SUPPORT ROLES		2
APPENDIX B: REFERENCES		2
APPENDIX C: SAMPLE DOCUMENTATION		2

List of Figures

Figure 1. <i>Matrix of Services and Related Support Roles</i>	2
---	---



NCR Interoperability Services (NCR-IS)

Security Policy

1 Purpose

The purpose of this document is to set forth policy for the secure establishment and operation of the National Capital Region Interoperability Services (NCR-IS). The intent of the controls recognized in this policy is to protect the confidentiality, integrity, and availability of the National Capital Region Interoperability Services (NCR-IS) and the information contained or exchanged by the NCR-IS with NCR-IS Partners.

This policy identifies the security measures needed to adequately protect the NCR-IS. This policy is not to be interpreted as an authority above existing governance structures, only to supplement them as relative to the NCR-IS Architecture.

2 Objectives

The objective of this policy is to describe the security controls which apply to the design and implementation of the NCR Interoperability Services and the day-to-day operations of the NCR-IS Architecture in achieving its stated mission objectives.

This security policy discusses requirements to facilitate a more consistent, comparable and repeatable approach for selecting and specifying security controls for the NCR-IS Architecture. Minimal security controls categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, should be adhered to.

Ultimately, this policy shall create a foundation for the development of assessment methods and procedures for determining security control effectiveness. The policies described in this document will promote a dynamic, extensible catalog of security controls for the National Capital Region Interoperability Services to more efficiently meet the demands of changing requirements and technologies.

3 Scope

This policy applies to the National Capital Region Interoperability Services (NCR-IS) and all interconnected logical and physical components owned by the NCR-IS. This consists of the personnel, technology, and operations supporting data exchanges, wireless and terrestrial networks between jurisdictions and/or mobile devices. This security policy does not address the security of components outside of the NCR-IS domain.

This policy applies to the protection of data at all security categorization levels *up to* the Sensitive but Unclassified (SBU) level.

Where circumstances prevent compliance with this policy, the NCR-IS shall document exceptions to this security policy where necessary to facilitate NCR-IS operations.

Given current NCR-IS installations at non-NCR-IS controlled facilities, the NCR-IS shall document exceptions to this security policy where necessary to comply with the security policies of non-NCR-IS controlled facilities.



NCR Interoperability Services (NCR-IS)

Security Policy

It is not the intent of this policy to impose or stipulate new requirements to which a jurisdiction must comply.

This policy clearly defines the relationship between the NCR-IS and the information exchanges between the NCR-IS Architecture and the NCR-IS Partner. The NCR-IS Architecture will not serve as the information owner of NCR-IS Partner data. The NCR-IS Partner is the information owner of the data and is responsible for the accuracy and integrity of the data or information exchanged with the NCR-IS Architecture. The NCR-IS Architecture in all responsibilities is the custodian of any data or information provided for allocation to varying jurisdictions also participating in exchanging information with the NCR-IS Architecture.

The NCR-IS is the agency responsible for deploying and managing computers, networks, and data storage. This policy provides details of what security measures are the responsibility of the NCR-IS and which measures are needed to adequately protect the operations of the NCR-IS Architecture in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

The NCR Interoperability Council (IC) shall be responsible for reviewing instances when consensus between the NCR-IS Partner and the NCR-IS Organization cannot be reached.

4 Roles and Responsibilities

For the purpose of this document, the roles and responsibilities have been determined by a set standard of job responsibilities, defined by the National Institute of Standards and Technology, National Capital Region, and all participating Jurisdictions, and define the roles and responsibilities relative to the NCR-IS Architecture. The descriptions of each job responsibility will not change; however, the titles are subject to change.

NCR-IS roles and responsibilities are common across the *NCR-IS Security Policy* (this document), the *Information Management Policy*, and the *NCR-IS Services Catalog*. They are included in this document in Appendices A and B.

5 Management Security Policy

5.1 Risk Assessment

5.1.1 Risk Assessment Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

NCR-IS Architecture ISOs and ISSOs shall work together to ensure that appropriate controls are in place and functioning to provide an adequate level of security to the extent authorized by law.



NCR Interoperability Services (NCR-IS)

Security Policy

5.1.2 Security Categorization

The NCR-IS CIO shall designate an NCR-IS ISSO within the NCR-IS to review and approve the security categorizations.

The NCR-IS ISSO, working with the NCR-IS ISO and NCR-IS Partner, shall categorize the information processed, stored, or transmitted by the system in accordance with appropriate levels of risk and document the results (including supporting rationale) in the NCR-IS System Security Plan (SSP).

During the system [risk assessment](#), the NCR-IS ISSO, working with the ISO and NCR-IS Partner, shall determine the sensitivity or violability of the NCR-IS Architecture to compromises in confidentiality, integrity, and availability of the information stored and processed by the system. The NCR-IS ISO and NCR-IS Partner are primarily responsible for identifying the [management](#), [technical](#), and [operational](#) controls appropriate to provide the required system and information protection.

5.1.3 Risk Assessment

The NCR-IS ISSO shall conduct a risk assessment of the NCR-IS Architecture and any interconnected data exchange at least every 3 years, or upon [significant change](#) to the NCR-IS Architecture. The NCR-IS ISSO shall conduct assessments of the level of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of NCR-IS resources and information. A significant change to the system includes any change to the system architecture, operating system, or information processing capabilities.

The NCR-IS Partner exchanging information with the NCR-IS Architecture is strongly recommended to conduct a risk assessment of the Information System that will be exchanging information with the NCR-IS Architecture.

The NCR-IS ISSO shall conduct a risk assessment on the interconnection between the NCR-IS Architecture and the NCR-IS Partner. This risk assessment shall be part of the formal Service Level Agreement (SLA) for the specific data exchange. Risk assessments will then be reviewed and validated by the NCR-IS CA prior to submission to the NCR-IS SAISO.

The NCR-IS CA shall identify and verify the levels of risk through conducting [assessment](#) of the security controls and evaluate whether they provide adequate security for NCR-IS Architecture and reduce the level of risk needed to obtain an Authority To Operate (ATO) by the NCR-IS AO. The NCR-IS CA identifies additional control needs, evaluates cost-effective solutions, and the [system owner](#) assigns resources to implement corrective action.

5.1.4 Vulnerability Assessment

Using appropriate vulnerability scanning tools and techniques, the NCR-IS CA shall scan for vulnerabilities within the NCR-IS Architecture at a specified frequency or when significant new vulnerabilities affecting the system are identified and reported. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The NCR-IS CA shall update the list of vulnerabilities within the NCR-IS Architecture at a specified frequency.



NCR Interoperability Services (NCR-IS)

Security Policy

5.2 Planning

5.2.1 Security Planning Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

The NCR-IS ISSO, working with the NCR-IS ISO and NCR-IS Partner, shall develop, disseminate and implement: (i) a formal, documented, NCR-IS Architecture System Security Plan (SSP)

5.2.2 System Security Plan

The NCR-IS Architecture ISSO, working with the NCR-IS ISO and NCR-IS Partner, shall develop, disseminate and implement: (i) a formal, documented, NCR-IS Architecture System Security Plan (SSP)

The NCR-IS SAISO shall review and approve the plan and determine the optimal place of the security function within the agency hierarchy with the shortest practicable reporting lines to the NCR-IS CIO or NCR-IS Agency Head.

The NCR-IS SAISO shall maintain documentation of the NCR-IS Architecture System Security Plan for review by NCR-IS Chief Information Officer as required.

5.2.3 Rules of Behavior

The NCR-IS Architecture ISSO shall establish and make readily available to all NCR-IS Architecture Users a set of rules that describes their responsibilities and expected behavior when using the NCR-IS.

NCR-IS ISSOs shall obtain signed acknowledgement documentation from NCR-IS Users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the NCR-IS Architecture.

5.3 System & Services Acquisition

5.3.1 System and Services Acquisition Policy and procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.



NCR Interoperability Services (NCR-IS)

Security Policy

5.3.2 Allocation of Resources

The NCR-IS CIO shall determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the NCR-IS Architecture.

5.3.3 Life Cycle Support

The NCR-IS ISO shall manage the NCR-IS Architecture using a system development life cycle methodology that includes information security considerations.

5.3.4 Acquisitions

The NCR-IS ISO shall include security requirements and/or security specifications, either explicitly or by reference, in NCR-IS Architecture acquisition contracts based on an assessment of risk.

The systems and services provided by contractors to the NCR-IS Architecture shall be governed by the security requirements and/or specifications identified by the NCR-IS ISO. Systems and services shall include all lifecycle activities including, but not limited to testing, quality control, installation, operation, and maintenance of computer equipment.

5.3.5 Documentation

The NCR-IS ISO shall ensure that adequate documentation for the NCR-IS Architecture and its constituent components are available, protected when required, and distributed to authorized personnel. The documentation shall minimally include a description of functional properties and as well as the design and implementation details (including functional interfaces among control components) of the security controls employed within the NCR-IS Architecture with sufficient detail to permit analysis and testing of the controls.

The NCR-IS internal website shall contain the most current approved version of the NCR-IS Security Policy with links to applicable standards, guidelines, procedures, and forms.

5.3.6 Software Usage Restrictions

All NCR-IS Users of the NCR-IS Architecture shall comply with software usage restrictions. The NCR-IS Architecture shall employ tracking systems to control copying and distribution for software and associated documentation protected by quantity licenses.

5.3.7 User Installed Software

The NCR-IS ISSO shall enforce explicit rules governing the downloading and installation of software by NCR-IS Users.

5.3.8 Security Design Principles

The NCR-IS ISO shall design and implement the NCR-IS Architecture using sound security engineering principles as defined by the National Institute of Standards and Technology.



5.3.9 Outsourced Services

The NCR-IS ISO shall ensure that third-party providers of NCR-IS Architecture services and NCR-IS Partners employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. Validation of compliance shall be enforced through continuous monitoring.

6 Operational Security Policy

6.1 Personnel Security

6.1.1 Personnel Security Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

The NCR-IS ISSO shall facilitate the communication process between the NCR-IS ISO and senior management personnel within organization on matters relevant to personnel security.

The NCR-IS ISSO shall be responsible for ensuring that each NCR-IS staff and contractor position is designated at the appropriate level of position sensitivity and/or risk. The NCR-IS ISSO shall also ensure that this designation is clearly stated in the employee's position description and that suitable background investigations are performed.

6.1.2 Position Categorization

The NCR-IS ISSO shall assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The NCR-IS ISSO shall also review and revise position risk designations at specified frequency or every three years.

Where feasible, the NCR-IS ISO and NCR-IS ISSO will [separate](#) sensitive duties to preclude any one individual from gaining the opportunity to adversely affect the NCR-IS Architecture. The NCR-IS [ISSO](#) will ensure that the NCR-IS ISO has defined procedural checks and balances for personnel security in the system security plan. The NCR-IS ISSO will ensure enforceability of these [controls](#) so accountability is established and security violations are detectable.

6.1.3 Personnel Screening

The NCR-IS ISO and NCR-IS ISSO shall screen individuals requiring access to organizational information before authorizing access.

Foreign nationals will not be granted access to or perform critical sensitive duties on the NCR-IS Architecture.



NCR Interoperability Services (NCR-IS)

Security Policy

The NCR-IS AO shall ensure that a risk-based, cost-effective approach is followed to determine the risk of harm to the NCR-IS Architecture in comparison to the opportunity to bypass system security control settings or those who have access to software source code.

6.1.4 Personnel Termination

When employment is terminated the NCR-IS System Administrator shall terminate access to the NCR-IS Architecture.

The NCR-IS ISSO shall conduct exit interviews, and ensure the return of all organizational NCR-IS Architecture-related property (e.g., keys, identification cards, building passes) in a timely manner.

The NCR-IS ISSO shall also ensure that appropriate personnel have access to official records created by the terminated employee that are stored within the NCR-IS Architecture before the systems are recycled or disposed.

6.1.5 Personnel Transfer

The NCR-IS ISSO shall review NCR-IS Architecture facility access authorizations when individuals are reassigned or transferred to other positions within the NCR-IS Architecture and initiate appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

The NCR-IS ISO and ISSO shall ensure that the NCR-IS Architecture maintains adequate controls for changes in user access (either between operating units or with regard to job duties).

6.1.6 Access Agreements

The NCR-IS User of the NCR-IS Architecture shall complete an appropriate access agreement (e.g., nondisclosure agreement, acceptable use agreement, rules of behavior, conflict-of-interest agreement) for all individuals requiring access before authorizing access.

Prior to establishing an account for access to the NCR-IS Architecture, the System Administrator shall ensure that each agreement is signed and dated.

6.1.7 Third-Party Personnel Security

The NCR-IS ISSO shall establish personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing NCR-IS Architecture development, information technology services, outsourced applications, and network and security management). Established security requirements shall be approved by the NCR-IS SAISO.

The NCR-IS ISSO shall monitor provider compliance to ensure adequate security.

6.1.8 Personnel Sanctions

The NCR-IS ISSO shall enforce formal sanctions, for personnel failing to comply with established NCR-IS Architecture security policies and procedures.



6.2 Physical & Environmental Protection

6.2.1 Physical and Environmental Protection Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

6.2.2 Physical Access Authorizations

The NCR-IS ISSO shall develop and keep current lists of personnel with authorized access to facilities within the NCR-IS Architecture (except for those areas within the facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards).

The NCR-IS Architecture ISSO shall review and approve the access list and authorization credentials at a specified frequency, at least annually.

6.2.3 Physical Access Control

The NCR-IS ISSO shall designate an officer to control all physical access points (including designated entry/exit points) to facilities within the NCR-IS Architecture (except for those areas within the facilities officially designated as publicly accessible) and verify individual access authorizations before granting access to the facilities.

6.2.4 Access Control for Display

NCR-IS Users shall control physical access to any NCR-IS Architecture device that displays information to prevent unauthorized individuals from observing the display output.

6.2.5 Monitoring Physical Access

The NCR-IS ISSO shall designate an officer to monitor physical access to the NCR-IS Architecture to detect and respond to incidents. The NCR-IS ISSO designated officer shall monitor real-time intrusion alarms and surveillance equipment and employ automated mechanisms to ensure potential intrusions are recognized and appropriate response actions are initiated.

6.2.6 Visitor Control

The NCR-IS SAISO shall provide a mechanism to control physical access to the NCR-IS Architecture by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. The NCR-IS Partner shall comply by ensuring visitors are escorted and activity monitored.



NCR Interoperability Services (NCR-IS)

Security Policy

6.2.7 Access Logs

The NCR-IS ISSO and the NCR-IS Partner shall maintain a visitor access log to facilities within the NCR-IS Architecture (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited.

The NCR-IS ISSO and the NCR-IS Partner shall review the access logs at a specified frequency after closeout.

The NCR-IS ISSO shall employ automated mechanisms to facilitate the maintenance and review of access logs.

6.2.8 Power Equipment and Power Cabling

The NCR-IS ISSO and the NCR-IS Partner shall ensure the protection of power equipment and power cabling for the NCR-IS Architecture from damage and destruction.

6.2.9 Emergency Shutoff

For specific locations within a facility containing concentrations of NCR-IS Architecture resources (e.g., data centers, server rooms, mainframe rooms), the NCR-IS ISSO and the NCR-IS Partner shall ensure the capability of shutting off power to any information technology component that may be malfunctioning without endangering personnel by requiring them to approach the equipment.

6.2.10 Emergency Power

The NCR-IS ISSO and the NCR-IS Partner shall ensure short-term uninterruptible power supply to facilitate an orderly shutdown of the NCR-IS Architecture in the event of a primary power source loss. In addition, the NCR-IS ISSO and NCR-IS Partner shall ensure a long-term alternate power supply for the NCR-IS Architecture that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

In the event of power loss the NCR-IS ISSO and the NCR-IS Partner shall be notified immediately upon loss of system use.

6.2.11 Fire Protection

The NCR-IS ISSO and the NCR-IS Partner shall ensure the employment and maintenance of fire suppression and detection devices/systems that can be activated automatically in the event of a fire. These fire suppression and detection devices/systems used shall provide automatic notification of any activation within the NCR-IS Architecture.

6.2.12 Temperature and Humidity Controls

The NCR-IS ISSO and NCR-IS Partner shall ensure facilities containing NCR-IS Architecture equipment are monitored and maintained within acceptable levels of temperature and humidity.



NCR Interoperability Services (NCR-IS)

Security Policy

6.2.13 Water Damage Protection

The NCR-IS ISSO and the NCR-IS Partner shall ensure all facilities containing NCR-IS Architecture equipment are adequately protected from water damage resulting from broken plumbing lines or other sources of water leakage and that a master shutoff valve is accessible, working properly, and known to key personnel. In the event of significant water leak automated mechanisms shall be employed to automatically close shutoff valves.

6.2.14 Delivery and Removal

The NCR-IS ISSO and the NCR-IS Partner shall control NCR-IS Architecture related items (i.e., hardware, firmware, software) entering and exiting the facility and maintain appropriate records of those items.

6.2.15 Alternate Work Site

The NCR-IS ISSO and the NCR-IS Partner shall employ appropriate NCR-IS Architecture security controls at alternate work sites.

6.3 Contingency Planning

6.3.1 Contingency Planning Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

6.3.2 Contingency Plan

The NCR-IS ISO shall develop and implement a contingency plan addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure.

The NCR-IS ISSO and NCR-IS SAISO shall review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

The NCR-IS SAISO shall coordinate contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan).

6.3.3 Contingency Training

The NCR-IS SAISO shall ensure all personnel are adequately trained in their contingency roles and responsibilities with respect to the NCR-IS Architecture. The NCR-IS SAISO shall also provide refresher training at specified frequency, at least annually while incorporating simulated events into contingency training to facilitate effective response by personnel in crisis situations.



NCR Interoperability Services (NCR-IS)

Security Policy

6.3.4 Contingency Plan Testing

The NCR-IS ISSO shall test the contingency plan at a specified frequency, at least annually using specified tests and exercises to determine the plan's effectiveness and the NCR-IS Architecture's readiness to execute the plan. The NCR-IS ISSO shall also test the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. The NCR-IS ISO shall then review the contingency plan test results and initiate corrective actions.

The NCR-IS SAISO shall coordinate contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan).

6.3.5 Alternate Storage Site

The NCR-IS ISO and NCR-IS Partner shall identify an alternate storage site and initiate necessary agreements to permit the storage of NCR-IS Architecture backup information. The transport of information from the primary storage site to the alternate storage site shall occur via a secure means of transfer. The alternate storage site shall be geographically separated from the primary storage site so as not to be susceptible to the same hazards and configured to facilitate timely and effective recovery operations.

The NCR-IS ISSO shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. A Memorandum of Understanding, Service Level Agreement, and Interconnection Agreement shall be instituted for each designated alternate processing site requirements when applicable.

6.3.6 Alternate Processing Site

The NCR-IS ISO shall identify an alternate processing site and initiate necessary agreements to permit the resumption of NCR-IS Architecture operations for critical mission/business functions within specified time period when the primary processing capabilities are unavailable. The alternate processing site shall be fully configured to support a minimum required operational capability and ready to use as the operational site. A designated alternate processing site shall be geographically separated from the primary processing site so as not to be susceptible to the same hazards.

The NCR-IS ISSO shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. A Memorandum of Understanding, Service Level Agreement, and Interconnection Agreement shall be instituted for each designated alternate processing site requirements.

6.3.7 Telecommunications Service

The NCR-IS ISO shall identify primary and alternate telecommunications services to support the NCR-IS Architecture and initiate necessary agreements to permit the resumption of system operations for critical mission/business functions within specified time period when the primary telecommunications capabilities are unavailable. The primary and alternate telecommunications



NCR Interoperability Services (NCR-IS)

Security Policy

service agreements should contain priority-of-service provisions in accordance with the organization's availability requirements.

The NCR-IS ISSO shall ensure that alternate telecommunications service providers to the NCR-IS Architecture are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

The NCR-IS ISSO shall ensure that adequate contingency plans for primary and alternate telecommunications service providers are instituted.

6.3.8 NCR-IS Architecture Backup

The NCR-IS ISO and the NCR-IS Partner shall ensure the archival of all data and metadata under their cognizant authority.

The NCR-IS ISO and the NCR-IS Partner shall conduct backups of user-level and system-level information (including system state information) contained in the NCR-IS Architecture at specified frequency. Backup information shall be stored at an appropriately secured location.

The NCR-IS ISO and the NCR-IS Partner shall test backup information at specified frequency to ensure media reliability and information integrity.

The NCR-IS ISO and the NCR-IS Partner shall selectively use backup information in the restoration of NCR-IS Architecture functions as part of contingency plan testing.

The NCR-IS ISO and the NCR-IS Partner shall ensure backup copies of the operating system and other critical NCR-IS Architecture software are stored in a separate facility or in a fire-rated container that is not collocated with the operational software, as approved by the NCR-IS SAISO.

6.3.9 NCR-IS Architecture Recovery and Reconstitution

The NCR-IS ISSO and the NCR-IS Partner shall employ mechanisms with supporting procedures to allow the NCR-IS Architecture to be recovered and reconstituted to the system's original state after a disruption or failure. Full recovery and reconstitution of the NCR-IS Architecture shall be included as part of contingency plan testing.

6.4 Configuration Management

6.4.1 Configuration Management Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

The NCR-IS ISO and NCR-IS ISSO shall identify configuration baselines for the item to be configured -- what the item is (e.g., system specifications, system or program documentation,



NCR Interoperability Services (NCR-IS)

Security Policy

or the set-up of a hardware or software component of a system), and assign the item a unique identifier such as a number or title and version number.

During configuration change control the NCR-IS ISO shall provide a request for recommended changes to an ISSO and NCR-IS SAISO in writing for approval. The NCR-IS ISO shall also ensure that approved changes are tested before implementation.

The NCR-IS ISSO shall track all approved changes to the NCR-IS Architecture and maintain documentation associated with authorized changes.

6.4.2 Baseline Configuration

The NCR-IS ISO, in partnership with the NCR-IS ISSO, shall develop, document, and maintain a current, baseline configuration of the NCR-IS Architecture and an inventory of the system's constituent components, update the baseline configuration as an integral part of NCR-IS Architecture component installations, and employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

6.4.3 Configuration Change Control

The NCR-IS ISSO shall document and control changes to the NCR-IS Architecture. The NCR-IS ISSO and NCR-IS SAISO shall approve NCR-IS Architecture changes in accordance with organizational policies and procedures.

The NCR-IS ISSO shall employ automated mechanisms to: (i) document proposed changes to the NCR-IS Architecture; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the NCR-IS Architecture.

6.4.4 Monitoring Configuration Changes

The NCR-IS ISSO shall monitor changes to the NCR-IS Architecture and conduct security impact analyses to determine the effects of the changes.

6.4.5 Access Restrictions for Change

The NCR-IS ISSO shall enforce access restrictions associated with changes to the NCR-IS Architecture. The ISSO shall also employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

6.4.6 Configuration Settings

The NCR-IS ISO shall configure the security settings of information technology products to the most restrictive mode consistent with NCR-IS Architecture operational requirements. The Technical Manager shall also employ automated mechanisms to centrally manage, apply, and verify configuration settings.



NCR Interoperability Services (NCR-IS)

Security Policy

6.4.7 Least Functionality

The NCR-IS ISO shall configure the NCR-IS Architecture to provide only essential capabilities and specifically prohibits and/or restricts the use of specified functions, ports, protocols, and/or services

The NCR-IS ISO shall review the NCR-IS Architecture at a specified frequency, to identify and eliminate unnecessary functions, ports, protocols, and/or services.

6.5 Maintenance

6.5.1 System Maintenance Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, NCR-IS Architecture maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the NCR-IS Architecture maintenance policy and associated system maintenance controls.

6.5.2 Periodic Maintenance

The NCR-IS ISO shall schedule, perform, and document routine preventative and regular maintenance on the components of the NCR-IS Architecture in accordance with manufacturer or vendor specifications and/or NCR-IS Architecture requirements. In addition, the NCR-IS ISO will maintain a log for the NCR-IS Architecture that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

The NCR-IS ISO shall employ automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

6.5.3 Maintenance Tools

The NCR-IS ISSO shall approve, control, and monitor the use of NCR-IS Architecture maintenance tools and maintain the tools on an ongoing basis.

The NCR-IS ISSO shall ensure the inspection of all NCR-IS Architecture maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

The NCR-IS ISSO shall ensure that all NCR-IS Architecture media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) is validated to be free of malicious code before the media are used in the NCR-IS Architecture.

The NCR-IS ISSO shall ensure that all maintenance equipment with the capability of retaining information is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the NCR-IS Architecture or is destroyed, unless an appropriate NCR-IS Architecture official explicitly authorizes an exception.



NCR Interoperability Services (NCR-IS)

Security Policy

6.5.4 Remote Maintenance

The NCR-IS ISSO shall approve, control, and monitor remotely executed maintenance and diagnostic activities, review the audit logs of the remote sessions, and address the installation and use of remote diagnostic links in the security plan for the NCR-IS Architecture.

The NCR-IS ISSO shall ensure that remote diagnostic or maintenance services within the NCR-IS Architecture implements the same level of security as that implemented on the NCR-IS Architecture being serviced.

6.5.5 Maintenance Personnel

The NCR-IS ISO shall maintain a list of personnel authorized to perform maintenance on the NCR-IS Architecture.

The NCR-IS ISO shall ensure that only authorized personnel perform maintenance on the NCR-IS Architecture and those personnel have appropriate access authorizations.

6.5.6 Timely Maintenance

The NCR-IS ISO shall obtain maintenance support and spare parts for specified list of key NCR-IS Architecture components within specified time period of failure.

6.6 System & Information Integrity

6.6.1 System and Information Integrity Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

6.6.2 Flaw Remediation

The NCR-IS ISO working with the ISSO shall identify, report, and correct NCR-IS Architecture flaws.

6.6.3 Malicious Code Protection

The NCR-IS Partner shall conduct malicious code protection prior to submitting data for exchange with the NCR-IS Architecture.

The NCR-IS ISO shall employ virus protection mechanisms at critical NCR-IS Architecture entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and also at workstations, servers, or mobile computing devices on the network.

The NCR-IS ISO shall also implement malicious code protection that includes a capability for automatic updates and ensure that the system will centrally manage virus protection mechanisms and automatically update virus protection mechanisms.



NCR Interoperability Services (NCR-IS)

Security Policy

6.6.4 Intrusion Detection Tools and Techniques

The NCR-IS ISO shall employ tools and techniques to monitor events on the NCR-IS Architecture, detect attacks, and provide identification of unauthorized use of the system.

6.6.5 Security Alerts and Advisories

The NCR-IS ISSO shall employ automated mechanisms to receive NCR-IS Architecture security alerts/advisories on a regular basis.

In the case of an alert, the NCR-IS ISSO shall issue alerts/advisories to the NCR-IS ISO, take appropriate actions in response and document the types of actions to be taken in response to security alerts/advisories. Appropriate actions shall include, at a minimum, the notification of impacted NCR-IS Partners.

6.6.6 Security Functionality Verification

The NCR-IS System Administrator shall verify the correct operation of NCR-IS security functions as designated at a specified frequency and react accordingly when anomalies are discovered. The NCR-IS System Administrator shall notify the NCR-IS ISO, prior to shutting the system down or restarting the system when anomalies are discovered. The NCR-IS ISO shall notify impacted NCR-IS Partners of anomalies which would affect one or more NCR-IS Partners.

The NCR-IS ISSO shall enforce automated mechanisms to provide notification of failed security tests.

6.6.7 Software and Information Integrity

The NCR-IS ISO shall ensure detection and protection against unauthorized changes to software and information.

The NCR-IS ISO shall employ integrity verification applications in the NCR-IS Architecture to monitor for information tampering, errors, and omissions.

6.6.8 Spam and Spyware Protection

The NCR-IS ISO shall ensure the implementation of spam and spyware protection that is centrally managed.

The NCR-IS ISO shall employ spam and spyware protection mechanisms at critical NCR-IS Architecture entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.

6.6.9 Information Input Restrictions (accuracy, completeness, and validity)

The NCR-IS ISO shall restrict the information input to the NCR-IS Architecture to authorized personnel only.



NCR Interoperability Services (NCR-IS)

Security Policy

6.6.10 Information Output Handling and Retention

The NCR-IS Partner shall ensure accuracy, completeness, and validity of information inputs submitted to the NCR-IS Architecture. The NCR-IS Architecture shall NOT be responsible for ensuring accuracy of data.

6.6.11 Error Handling

The NCR-IS ISO shall ensure that error conditions are identified and handled in an expeditious manner.

6.6.12 Information Output Handling and Retention

The NCR-IS ISO shall ensure the proper handling and output, of NCR-IS Architecture information.

The NCR-IS Partner shall ensure the proper retention of information under their authority.

6.7 Media Protection

6.7.1 Media Protection Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

6.7.2 Media Access

The NCR-IS ISO and NCR-IS Partner shall provide the NCR-IS Architecture with a comprehensive outline that clearly defines the level of access granted to NCR-IS Users based on roles and responsibilities as described in this NCR-IS Security Policy.

The NCR-IS ISO shall ensure that only authorized NCR-IS users have access to information in printed form or on digital media removed from the NCR-IS Architecture.

Unless guard stations control access to media storage areas, the NCR-IS ISSO shall employ automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.

6.7.3 Media Labeling

The NCR-IS ISO and NCR-IS Partner shall accurately categorize and label all electronic files, hard copy printouts, and removable media (diskettes and CD-ROMs) containing data categorized as For (FOUO), U.S. Code Title or Public Law protected data, or national security information (confidential, secret, top secret, or other designation).



NCR Interoperability Services (NCR-IS)

Security Policy

The NCR-IS ISO and NCR-IS Partner shall affix external labels to removable information storage media and NCR-IS Architecture output indicating the distribution limitations and handling caveats of the information.

6.7.4 Media Storage

The NCR-IS ISO and the NCR-IS Partner shall ensure that NCR-IS Architecture media storage is physically controlled and securely stored, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.

6.7.5 Media Transport

The NCR-IS ISO and the NCR-IS Partner shall control NCR-IS Architecture media (paper and digital) and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

6.7.6 Media Sanitization

The ISO and the NCR-IS Partner shall ensure the proper sanitization of media, where appropriated.

6.7.7 Media Destruction and Disposal

The NCR-IS ISO and the NCR-IS Partner shall sanitize or destroy NCR-IS Architecture digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using the information contained on the media.

6.8 Incident Response

6.8.1 Incident Response Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

The NCR-IS ISO and each NCR-IS Partner shall have a written MOU for support required to effectively monitor, respond, report, and prevent [incidents](#) occurring during exchanges with the NCR-IS Architecture. This includes the communication of incident information to NCR-IS Partners by NCR-IS personnel.

NCR-IS Users shall report security [incidents](#), suspected or otherwise, to the NCR-IS ISSO. In turn, the ISSO should provide all relevant security to the NCR-IS ISO and NCR-IS SAISO. The NCR-IS ISO shall communicate incident information to impacted NCR-IS Partners.

The NCR-IS ISSO shall take appropriate actions, when incidents are reported, to determine whether a violation of a Rule of Behavior has occurred and with further investigation is necessary.



NCR Interoperability Services (NCR-IS)

Security Policy

6.8.2 Incident Response Training

The NCR-IS SAISO shall ensure adequate training for personnel in their incident response roles and responsibilities with respect to the NCR-IS Architecture and provide refresher training at specified frequency, at least annually.

The NCR-IS SAISO shall ensure that simulated events are incorporated into NCR-IS Architecture incident response training to facilitate effective response by personnel in crisis situations.

6.8.3 Incident Response Testing

The NCR-IS ISSO shall test the NCR-IS Architecture incident response capability at specified frequency, at least annually using specified tests and exercises to determine the incident response effectiveness and document the results.

The NCR-IS ISSO shall employ automated mechanisms to more thoroughly and effectively test the incident response capability.

6.8.4 Incident Handling

The NCR-IS ISSO shall ensure the implementation of an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

The NCR-IS ISSO shall also employ automated mechanisms to support the incident handling process.

6.8.5 Incident Monitoring

The NCR-IS ISSO shall track and document NCR-IS Architecture security incidents on an ongoing basis and employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

6.8.6 Incident Reporting

NCR-IS Users of the NCR-IS Architecture shall report incident information to the ISSO. The ISSO shall accept incident information from NCR-IS Partners.

The NCR-IS ISSO shall employ automated mechanisms to assist in the reporting of security incidents. The NCR-IS ISSO shall employ available mechanisms, automated or otherwise, to report incident information to impacted NCR-IS Partners.

The NCR-IS ISO shall document a common set of terms and relationships between those terms such as event an occurrence that the system recognizes (such as multiple password attempts) or adverse event (an event with negative consequences).



NCR Interoperability Services (NCR-IS)

Security Policy

6.8.7 Incident Response Assistance

The NCR-IS ISSO shall ensure the availability of an incident response support resource that offers advice and assistance to Users of the NCR-IS Architecture for the handling and reporting of security incidents. The support resource shall be an integral part of the organization's incident response capability.

The NCR-IS ISSO shall ensure the implementation of automated mechanisms to increase the availability of incident response-related information and support.

6.9 Security Awareness Training

6.9.1 Security Awareness and Training Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

6.9.2 Security Awareness

The NCR-IS SAISO shall ensure all NCR-IS staff and contractors are exposed to basic NCR-IS Architecture security awareness materials before authorizing access to the system and on an annual basis thereafter.

6.9.3 Security Training

The NCR-IS ISO shall identify personnel with significant NCR-IS Architecture security roles and responsibilities and then provide documentation of those roles and responsibilities.

The NCR-IS SAISO shall ensure appropriate NCR-IS Architecture security training is available to NCR-IS Users before authorizing access to the system and periodically thereafter.

6.9.4 Security Training Records

The NCR-IS ISSO shall document and monitor individual NCR-IS Architecture security training activities including basic security awareness training and specific NCR-IS Architecture security training.



7 Technical Security Policy

7.1 Identification & Authentication

7.1.1 Identification and Authentication Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

7.1.2 User Identification and Authentication

The NCR-IS ISO shall ensure unique identification and authentication of NCR-IS Users (or processes acting on behalf of users) and that each employ multifactor authentication. The NCR-IS ISO shall ensure the NCR-IS Architecture can support identification and authentication needs set forth in Service Level Agreements.

The NCR-IS ISO shall employ a “forgot password” capability that maintains the level of access requirements set forth in the NCR-IS Security Policy.

7.1.3 Device Identification and Authentication

The NCR-IS ISO shall ensure the proper identification and authentication of specific devices before establishing a connection. This includes the establishment of appropriate controls and methods to identify and authenticate NCR-IS Partner information systems for the purposes of data exchange.

7.1.4 Identifier Management

The NCR-IS ISO shall ensure the management of user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after specified period of inactivity; and (vi) archiving user identifiers.

7.1.5 Authenticator Management

The NCR-IS ISO shall ensure the management of NCR-IS Architecture authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon NCR-IS Architecture installation.



NCR Interoperability Services (NCR-IS)

Security Policy

7.1.6 Authentication Feedback

The NCR-IS ISO shall ensure NCR-IS Users are provided feedback during an attempted authentication and that such feedback shall not compromise the authentication mechanism.

7.1.7 Cryptographic Module Authentication

The NCR-IS ISO shall ensure the NCR-IS Architecture employs cryptographic authentication methods that meet the requirements designated by the National Institute of Standards and Technology.

7.2 Access Control

7.2.1 Access Control Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

The NCR-IS ISO shall authorize and enforce a user's access to and action towards specified resources based on least privilege. All accounts created shall have an associated formal request forms with approvals that is appropriate for the NCR-IS Architecture service.

The NCR-IS ISO shall authorize all special access accounts required for audit, software development, software installation, or other defined need.

The NCR-IS System Administrator shall ensure accounts are authorized, created with a specific expiration date, and be removed immediately when work is complete.

7.2.2 Account Management

Under the authority of the NCR-IS ISO, the System Administrator shall manage NCR-IS Architecture accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

The NCR-IS System Administrator shall set controls for the automatic termination of temporary and emergency accounts after specified period of time and shall also ensure the immediate disabling of inactive accounts within the specified period of time.

The NCR-IS ISSO shall employ automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

The NCR-IS ISSO shall review NCR-IS Architecture accounts periodically and employ automated mechanisms to support the management of NCR-IS Architecture accounts.



NCR Interoperability Services (NCR-IS)

Security Policy

7.2.3 Access Enforcement

The NCR-IS ISO shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

The NCR-IS ISO shall ensure that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

The NCR-IS ISO shall ensure the cryptographic devices employ NIST FIPS 140-2 compliance for encryption.

7.2.4 Information Flow Enforcement

The NCR-IS ISSO, working with the ISO, shall enforce assigned authorizations, as authorized by the NCR-IS SAISO, for controlling the flow of information within the NCR-IS Architecture and between data exchanges in accordance with applicable policy.

7.2.5 Separation of Duties

The NCR-IS ISO shall enforce separation of duties through assigned access authorizations. Separation of duties shall occur between NCR-IS System Administrator, NCR-IS Certification Agent, and the NCR-IS Information System Security Officer.

7.2.6 Least Privilege

The NCR-IS ISO shall enforce the most restrictive set of rights/privileges or accesses needed by NCR-IS Users (or processes acting on behalf of users) for the performance of specified tasks.

7.2.7 Unsuccessful Login Attempts

The NCR-IS System Administrator shall ensure a limit of consecutive invalid access attempts by a user during a defined time period.

The NCR-IS System Administrator shall ensure NCR-IS Architecture locks out the account for a pre-set time period of at least 15 minutes after which it can automatically reset.

The NCR-IS System Administrator shall ensure locked accounts with privileged access (i.e., root access) will remain locked until unlocked by the NCR-IS System Administrator. Reasonable and verifiable means of identification will be required to request an account be unlocked and specified in processes and procedures outside of this document.

7.2.8 System Use Notification

The NCR-IS ISO shall ensure the display an approved, system use notification message before granting system access informing potential NCR-IS and NCR-IS Partner Users: (i) that the user is accessing a the NCR-IS; (ii) that system usage may be monitored, recorded, and subject to



NCR Interoperability Services (NCR-IS)

Security Policy

audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording.

The NCR-IS ISO shall ensure the use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user takes explicit actions to log on to the NCR-IS Architecture.

7.2.9 Concurrent Session Lock

The NCR-IS System Administrator shall limit the number of concurrent sessions for any user to specified number of sessions.

7.2.10 Session Lock

The NCR-IS System Administrator shall ensure prevention of further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

7.2.11 Session Termination

The NCR-IS System Administrator shall ensure automatic termination of a session after a specified period of inactivity.

7.2.12 Supervision and Review – Access Control

The NCR-IS ISSO shall ensure the supervision and review the activities of NCR-IS and NCR-IS Partner Users with respect to the enforcement and usage of NCR-IS Architecture access controls.

The NCR-IS ISSO shall ensure the implementation of automated mechanisms to facilitate the review of NCR-IS and NCR-IS Partner User activities.

7.2.13 Permitted Actions without Identification and Authentication

The NCR-IS ISO shall identify specific user actions that can be performed on the NCR-IS Architecture without identification or authentication and permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

7.2.14 Automated Marking

The NCR-IS PARTNER shall ensure marked output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

7.2.15 Remote Access

The NCR-IS ISO shall document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the NCR-IS Architecture including remote access for privileged functions.



NCR Interoperability Services (NCR-IS)

Security Policy

The NCR-IS ISO shall authorize each remote access method and authorize only the necessary NCR-IS Users for each access method.

The NCR-IS ISSO shall ensure automated mechanisms to facilitate the monitoring and control of remote access methods, use encryption to protect the confidentiality of remote access sessions, and control all remote accesses through a managed access control point.

The NCR-IS shall restrict the use of a secured network connection such that the system security controls are not bypassed.

7.2.16 Wireless Access Restrictions

The NCR-IS ISSO, working in conjunction with the ISO of each NCR Jurisdiction, shall establish usage restrictions and implementation guidance for wireless technologies.

The NCR-IS ISO, working in conjunction with the ISO of each NCR Jurisdiction, shall document, monitor, and control wireless access to the NCR-IS Architecture.

The NCR-IS ISO, working in conjunction with the ISO of each NCR Jurisdiction, shall ensure the use of authentication and encryption to protect wireless access to the NCR-IS Architecture.

The NCR-IS, working in conjunction with the ISO of each NCR Jurisdiction, shall employ security controls to restrict the ability to connect to more than one wireless data network.

The NCR-IS IC shall review all situations involving access restrictions for wireless technologies, where a consensus between the NCR-IS ISO and the NCR Jurisdiction ISOs cannot be reached.

7.2.17 Access Control for Portable and Mobile Devices

The NCR-IS ISSO shall establish usage restrictions and implementation guidance for portable and mobile devices and document, monitor, and control device access to the NCR-IS Architecture.

The NCR-IS ISO shall employ removable hard drives or cryptography to protect information residing on portable and mobile devices.

The NCR-IS ISO shall employ logical device locking mechanisms inherent to a portable or mobile device to restrict access to the device.

7.2.18 Personally Owned NCR-IS Architectures

The NCR-IS ISSO shall restrict the use of personally owned information systems for official NCR-IS Architecture business involving the processing, storage, or transmission of data contained within the NCR-IS Architecture.



7.3 Audit & Accountability

7.3.1 Audit and Accountability Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

7.3.2 Auditable Events

The NCR-IS ISO shall ensure the generation of audit records for the specified events.

7.3.3 Content of Audit Records

The NCR-IS ISO shall ensure the capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. Different audit trails may be used concurrently such as an event-oriented log and/or by keystroke monitoring.

The NCR-IS ISO shall ensure the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

The NCR-IS ISSO shall ensure the capability to centrally manage the content of audit records generated by individual components throughout the system.

7.3.4 Audit Storage Capacity

The NCR-IS ISO shall ensure the allocation of sufficient audit record storage capacity and configure auditing to prevent such capacity being exceeded.

7.3.5 Audit Processing

The NCR-IS ISO shall ensure the NCR-IS Architecture has a mechanism for alerting the NCR-IS System Administrator and ISSO, in the event of an audit failure or audit storage capacity being reached. In such an event the ISO shall take specified actions to ensure the complete recovery of audit records.

The NCR-IS ISO shall ensure the NCR-IS Architecture provides a warning when allocated audit record storage volume reaches specified percentage of maximum audit record storage capacity.

7.3.6 Audit Monitoring, Analysis, and Reporting

The NCR-IS ISSO shall ensure the regular review and analysis of audit records for indications of inappropriate or unusual activity; investigate suspicious activity or suspected violations; report findings to appropriate officials; and takes necessary actions.



NCR Interoperability Services (NCR-IS)

Security Policy

The NCR-IS ISSO shall ensure the NCR-IS Architecture employs an automated mechanism to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

7.3.7 Audit Reduction and Report Generation.

The NCR-IS ISO shall ensure the NCR-IS Architecture provides an audit reduction and report generation capability and the capability to automatically process audit records for events of interest based upon selectable, event criteria.

7.3.8 Time Stamps

The NCR-IS Architecture ISO shall ensure that NCR-IS Architecture provides time stamps for use in audit record generation.

7.3.9 Protection of Audit Information

The NCR-IS Architecture ISO shall ensure that the NCR-IS Architecture provides adequate protection of audit information and audit tools from unauthorized access, modification, and deletion.

7.3.10 Audit Retention

The NCR-IS ISO shall ensure that audit logs are retained for specified periods of time to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

7.4 System & Communication Protection

7.4.1 System and Communications Protection Policy and Procedures

The NCR-IS CIO shall develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

7.4.2 Application Partitioning

The NCR-IS ISO shall ensure the separation of user functionality (including user interface services) from NCR-IS Architecture management functionality.

7.4.3 Security Function Isolation

The NCR-IS ISO shall ensure that the NCR-IS Architecture isolates security functions from non-security functions.



NCR Interoperability Services (NCR-IS)

Security Policy

7.4.4 Information Remnants

The NCR-IS ISO shall ensure that the NCR-IS Architecture prevents unauthorized and unintended information transfer via shared system resources.

7.4.5 Denial of Service

The NCR-IS ISO shall ensure the NCR-IS Architecture protects against or limit the effects of specified types of denial of service attacks.

The NCR-IS ISO shall ensure the NCR-IS Architecture adequately manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

7.4.6 Resource Priority

The NCR-IS ISO shall ensure the NCR-IS Architecture limits the use of resources by priority.

The NCR-IS ISO shall implement and maintain procedures that ensure NCR-IS Architecture resources are protected in accordance with the provisions of applicable State and Federal law, State policy, policy and standards.

7.4.7 Boundary Protection

The NCR-IS ISO shall ensure the NCR-IS Architecture monitors and controls communications at the external boundary of the NCR-IS Architecture and at key internal boundaries within the system.

The NCR-IS ISO shall ensure the NCR-IS Architecture physically allocates publicly accessible NCR-IS Architecture components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces and prevent public access into the organization's internal networks except as appropriately mediated.

The NCR-IS ISO shall ensure the NCR-IS Architecture uses logical security controls to protect NCR-IS Architecture components from network disruptions.

7.4.8 Transmission Integrity

The NCR-IS ISO shall ensure NCR-IS Architecture protects the integrity of transmitted information and employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

7.4.9 Transmission Confidentiality

The NCR-IS ISO shall ensure the NCR-IS Architecture protects the confidentiality of transmitted information and employs cryptographic mechanisms to prevent unauthorized



NCR Interoperability Services (NCR-IS)

Security Policy

disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

7.4.10 Network Disconnect

The NCR-IS ISO shall ensure the NCR-IS Architecture terminates a network connection at the end of a session or after specified period of inactivity.

7.4.11 Cryptographic Key Establishment and Management

The NCR-IS ISO shall ensure the NCR-IS Architecture employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

7.4.12 Use of Validated Cryptography

The NCR-IS ISO shall ensure the NCR-IS Architecture performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

7.4.13 Public Access Protections

The NCR-IS ISO shall ensure the NCR-IS Architecture shall protect the integrity of the information and applications within public service zones.

7.4.14 Collaborative Computing

The NCR-IS ISO shall ensure the NCR-IS Architecture prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provide an explicit indication of use to the local NCR-IS Users (e.g., use of camera or microphone).

7.4.15 Public Key Infrastructure Certificates

The NCR-IS ISO shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the NCR-IS Architecture.

7.4.16 Mobile Code

The NCR-IS ISO shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the NCR-IS Architecture if used maliciously.

The NCR-IS ISO, working with the ISSO, shall document, monitor, and control the use of mobile code within the NCR-IS Architecture.

The NCR-IS AO, under the recommendation of the NCR-IS SAISO, shall remain the sole authority for authorizing the use of mobile code.



NCR Interoperability Services (NCR-IS)

Security Policy

7.4.17 Voice Over Internet Protocol

The NCR-IS ISO, working in conjunction with the Jurisdiction ISO, shall establish usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the NCR-IS Architecture if used maliciously.

The NCR-IS IC shall review all situations involving VOIP, where a consensus between the NCR-IS ISO and the Jurisdiction ISO cannot be reached.

The NCR-IS ISSO shall document, monitor, and control the use of VOIP within the NCR-IS Architecture.

The NCR-IS AO, under the recommendation of the NCR-IS SAISO, shall remain the sole authority for authorizing the use of VOIP.

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.

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).



NCR Interoperability Services (NCR-IS)

Security Policy

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)¹.

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 (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 (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.

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.

¹ 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)

Security Policy

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).

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.



NCR Interoperability Services (NCR-IS)

Security Policy

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.

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.



NCR Interoperability Services (NCR-IS)

Security Policy

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.

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.



NCR Interoperability Services (NCR-IS)

Security Policy

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).



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 has been determined that there are vulnerabilities, the NCR-IS CA provides recommended



NCR Interoperability Services (NCR-IS)

Security Policy

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)

Security 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 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.



NCR Interoperability Services (NCR-IS)

Security Policy

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.



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)

Security 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	<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	<p style="text-align: center;">Out-Sourcing Required for Interim M & O Period March – July 2007</p>																	
		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 B: References

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

1. County of Fairfax, Virginia, Fairfax County Policy & Procedures; Information Technology Security Policy, rev. 1: Department of Information Technology, April 2003.
2. Federal Information Security Management Act of 2002 (Public Law 107-347, Title III): December 2002.
3. Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems: February 2004.
4. Federal Information Processing Standards Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors: February, 2005.
5. Information Technology Infrastructure Library, Planning to Implement Service Management: Office of Government Commerce, 2002.
6. Merriam-Webster; www.m-w.com
7. National Institute of Standards and Technology Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995.
8. National Institute of Standards and Technology Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172): April 1998.
9. National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems: December 1998.
10. National Institute of Standards and Technology Special Publication 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products: August 2000.
11. National Institute of Standards and Technology Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems: November 2001.
12. National Institute of Standards and Technology Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security); Revision A: June 2004.
13. National Institute of Standards and Technology Special Publication 800-28, Guidelines on Active Content and Mobile Code: October 2001.
14. National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems: July 2002.
15. National Institute of Standards and Technology Special Publication 800-34, Contingency Planning Guide for Information Technology Systems: June 2002.
16. National Institute of Standards and Technology Special Publication 800-35, Guide to Information Technology Security Services: October 2003.
17. National Institute of Standards and Technology Special Publication 800-36, Guide to Selecting Information Security Products: October 2003.



NCR Interoperability Services (NCR-IS)

Security Policy

18. National Institute of Standards and Technology Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems: May 2004.
19. National Institute of Standards and Technology Special Publication 800-40, Procedures for Handling Security Patches: August 2002.
20. National Institute of Standards and Technology Special Publication 800-42, Guideline on Network Security Testing: October 2003.
21. National Institute of Standards and Technology Special Publication 800-46, Security for Telecommuting and Broadband Communications: August 2002.
22. National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems: August 2002.
23. National Institute of Standards and Technology Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices: November 2002.
24. National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program: October 2003.
25. National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems: February 2005.
26. National Institute of Standards and Technology Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems: April 2006.
27. Annex 1: National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems; Minimum Security Controls: June, 2005.
28. National Institute of Standards and Technology Special Publication 800-56, Recommendation on Key Establishment Schemes: January 2003.
29. National Institute of Standards and Technology Special Publication 800-57, Recommendation on Key Management: August 2005.
30. National Institute of Standards and Technology Special Publication 800-58, Security Considerations for Voice Over IP Systems: January 2005.
31. National Institute of Standards and Technology Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories: June 2004.
32. National Institute of Standards and Technology Special Publication 800-61, Computer Security Incident Handling Guide: January 2004.
33. National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology: April 2006.
34. National Institute of Standards and Technology Special Publication 800-64, Revision 1, Security Considerations in the Information System Development Life Cycle: June 2004.
35. National Institute of Standards and Technology Special Publication 800-65, Integrating Security into the Capital Planning and Investment Control Process: January 2005.



NCR Interoperability Services (NCR-IS)

Security Policy

36. National Institute of Standards and Technology Special Publication 800-70, Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers: May 2005.
37. National Institute of Standards and Technology Special Publication 800-73, Interfaces for Personal Identity Verification: March 2006.
38. National Institute of Standards and Technology Special Publication 800-76, Biometric Data Specification for Personal Identity Verification: February 2006.
39. National Security Telecommunications and Information Systems Security (No. 7003), Protective Distribution Systems (PDS): December 1996.
40. Office of Management and Budget, Memorandum M-03-22; OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
41. OPM Policy, Regulations, and Guidance; <http://www.opm.gov/index.asp>
42. The Dictionary of Homeland Security and Defense, p306, Margaret R. O'Leary: iUniverse, Inc.; March, 2006.
43. U.S. Department of Commerce, DOT IT Security Program Policy and Minimum Implementation Standards: DOC Information Technology, June 2005.
44. Wikipedia; www.wikipedia.com



Appendix C: Sample Documentation

Samples of the following documents are available upon request:

- ❖ System Security Plan
- ❖ Risk Assessment Sample
- ❖ Interconnection Security Agreement.