



Interoperable Communications Infrastructure (ICI) Security Policy

V2.0

July 2011

**Prepared by the
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.



Interoperable Communications Infrastructure

Security Policy

Revision History

Date	Description	Revisions Performed	Authorized by
12/07/2006	Beta v.5	See ARC Regional Security Policy Feedback documentation	ARC
7/30/2007	Beta v.6	See Metro CIO Regional Security Policy Feedback documentation; Revisions to role names after review of Regional SON	Metro CIO Committee
10/18/2007	v1.0	Revisions incorporated and approved – v1.0 for distribution	CIO Committee
02/03/2011	Beta v 1.0	Updated Policy based on adoption of ICI Security Practices and Procedures, and newly formed ICI.	ICI Program Support Staff
04/05/2011	v 2.0	Recommended for adoption by ICI Chief Information Security Officers (CISO) Committee	CISO Committee
07/21/2011	v2.0	Adopted and approved-v2.0 for distribution	CIO Committee



Executive Summary

The National Capital Region (NCR) Interoperable Communications Infrastructure (ICI) shall be responsible for transporting data, in the form of voice, text, images, and video, between ICI member 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 ICI member jurisdictions.

The ICI 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 ICI security policy, along with supporting practices and procedures, sets forth policy for the secure establishment and operation of the ICI. The intent of the controls recognized in this policy is to protect the confidentiality, integrity, and availability of the ICI and the information contained or exchanged by the ICI with ICI Partners.

The structure of the security policy follows publicly-available documentation from the National Institute of Standards and Technology and existing security policies of ICI-member jurisdictions. The policy uses the established ICI 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 ICI to be managed, operated and maintained.

Ultimately, this policy shall create a foundation for the development of security risk assessment methods, practices, and procedures for determining the security control effectiveness for new and existing ICI systems or applications.



Interoperable Communications Infrastructure

Security Policy

Table of Contents

1	PURPOSE	1
2	OBJECTIVES	1
3	SCOPE	1
4	ROLES AND RESPONSIBILITIES	3
5	MANAGEMENT SECURITY POLICY	5
5.1	RISK ASSESSMENT	5
5.1.1	<i>Risk Assessment Policy and Procedures</i>	5
5.1.2	<i>Security Categorization</i>	5
5.1.3	<i>Risk Assessment</i>	5
5.1.4	<i>Vulnerability Assessment</i>	6
5.2	PLANNING	6
5.2.1	<i>Security Planning Policy and Procedures</i>	6
5.2.2	<i>System Security Plan</i>	7
5.2.3	<i>Rules of Behavior</i>	7
5.3	SYSTEM & SERVICES ACQUISITION	7
5.3.1	<i>System and Services Acquisition Policy and procedures</i>	7
5.3.2	<i>Allocation of Resources</i>	7
5.3.3	<i>Life Cycle Support</i>	8
5.3.4	<i>Acquisitions</i>	8
5.3.5	<i>Documentation</i>	8
5.3.6	<i>Software Usage Restrictions</i>	8
5.3.7	<i>User Installed Software</i>	8
5.3.8	<i>Security Design Principles</i>	8
5.3.9	<i>Outsourced Services</i>	9
6	OPERATIONAL SECURITY POLICY	9
6.1	PERSONNEL SECURITY	9
6.1.1	<i>Personnel Security Policy and Procedures</i>	9
6.1.2	<i>Position Categorization</i>	9
6.1.3	<i>Personnel Screening</i>	9
6.1.4	<i>Personnel Termination</i>	10
6.1.5	<i>Personnel Transfer</i>	10
6.1.6	<i>Access Agreements</i>	10
6.1.7	<i>Third-Party Personnel Security</i>	10
6.1.8	<i>Personnel Sanctions</i>	11
6.2	PHYSICAL & ENVIRONMENTAL PROTECTION	11
6.2.1	<i>Physical and Environmental Protection Policy and Procedures</i>	11
6.2.2	<i>Physical Access Authorizations</i>	11
6.2.3	<i>Physical Access Control</i>	11
6.2.4	<i>Access Control for Display</i>	11
6.2.5	<i>Monitoring Physical Access</i>	11
6.2.6	<i>Visitor Control</i>	12
6.2.7	<i>Access Logs</i>	12
6.2.8	<i>Power Equipment and Power Cabling</i>	12
6.2.9	<i>Emergency Shutoff</i>	12
6.2.10	<i>Emergency Power</i>	12
6.2.11	<i>Fire Protection</i>	13



Interoperable Communications Infrastructure

Security Policy

6.2.12	Temperature and Humidity Controls.....	13
6.2.13	Water Damage Protection.....	13
6.2.14	Delivery and Removal.....	13
6.2.15	Alternate Work Site.....	13
6.3	CONTINGENCY PLANNING.....	13
6.3.1	Contingency Planning Policy and Procedures.....	13
6.3.2	Contingency Plan.....	13
6.3.3	Contingency Training.....	14
6.3.4	Contingency Plan Testing.....	14
6.3.5	Alternate Storage Site.....	14
6.3.6	Alternate Processing Site.....	14
6.3.7	Telecommunications Service.....	15
6.3.8	ICI Architecture Backup.....	15
6.3.9	ICI Architecture Recovery and Reconstitution.....	15
6.4	CONFIGURATION MANAGEMENT.....	16
6.4.1	Configuration Management Policy and Procedures.....	16
6.4.2	Baseline Configuration.....	16
6.4.3	Configuration Change Control.....	16
6.4.4	Monitoring Configuration Changes.....	17
6.4.5	Access Restrictions for Change.....	17
6.4.6	Configuration Settings.....	17
6.4.7	Least Functionality.....	17
6.5	MAINTENANCE.....	17
6.5.1	System Maintenance Policy and Procedures.....	17
6.5.2	Periodic Maintenance.....	17
6.5.3	Maintenance Tools.....	18
6.5.4	Remote Maintenance.....	18
6.5.5	Maintenance Personnel.....	18
6.5.6	Timely Maintenance.....	18
6.6	SYSTEM & INFORMATION INTEGRITY.....	19
6.6.1	System and Information Integrity Policy and Procedures.....	19
6.6.2	Flaw Remediation.....	19
6.6.3	Malicious Code Protection.....	19
6.6.4	Intrusion Detection Tools and Techniques.....	19
6.6.5	Security Alerts and Advisories.....	19
6.6.6	Security Functionality Verification.....	20
6.6.7	Software and Information Integrity.....	20
6.6.8	Spam and Spyware Protection.....	20
6.6.9	Information Input Restrictions (accuracy, completeness, and validity).....	20
6.6.10	Information Output Handling and Retention.....	20
6.6.11	Error Handling.....	20
6.6.12	Information Output Handling and Retention.....	21
6.7	MEDIA PROTECTION.....	21
6.7.1	Media Protection Policy and Procedures.....	21
6.7.2	Media Access.....	21
6.7.3	Media Labeling.....	21
6.7.4	Media Storage.....	21
6.7.5	Media Transport.....	22
6.7.6	Media Sanitization.....	22
6.7.7	Media Destruction and Disposal.....	22
6.8	INCIDENT RESPONSE.....	22
6.8.1	Incident Response Policy and Procedures.....	22
6.8.2	Incident Response Training.....	22



Interoperable Communications Infrastructure

Security Policy

6.8.3	<i>Incident Response Testing</i>	23
6.8.4	<i>Incident Handling</i>	23
6.8.5	<i>Incident Monitoring</i>	23
6.8.6	<i>Incident Reporting</i>	23
6.8.7	<i>Incident Response Assistance</i>	23
6.9	SECURITY AWARENESS TRAINING	24
6.9.1	<i>Security Awareness and Training Policy and Procedures</i>	24
6.9.2	<i>Security Awareness</i>	24
6.9.3	<i>Security Training</i>	24
6.9.4	<i>Security Training Records</i>	24
7	TECHNICAL SECURITY POLICY	25
7.1	IDENTIFICATION & AUTHENTICATION	25
7.1.1	<i>Identification and Authentication Policy and Procedures</i>	25
7.1.2	<i>User Identification and Authentication</i>	25
7.1.3	<i>Device Identification and Authentication</i>	25
7.1.4	<i>Identifier Management</i>	25
7.1.5	<i>Authenticator Management</i>	25
7.1.6	<i>Authentication Feedback</i>	26
7.1.7	<i>Cryptographic Module Authentication</i>	26
7.2	ACCESS CONTROL	26
7.2.1	<i>Access Control Policy and Procedures</i>	26
7.2.2	<i>Account Management</i>	26
7.2.3	<i>Access Enforcement</i>	27
7.2.4	<i>Information Flow Enforcement</i>	27
7.2.5	<i>Separation of Duties</i>	27
7.2.6	<i>Least Privilege</i>	27
7.2.7	<i>Unsuccessful Login Attempts</i>	27
7.2.8	<i>System Use Notification</i>	28
7.2.9	<i>Concurrent Session Lock</i>	28
7.2.10	<i>Session Lock</i>	28
7.2.11	<i>Session Termination</i>	28
7.2.12	<i>Supervision and Review – Access Control</i>	28
7.2.13	<i>Permitted Actions without Identification and Authentication</i>	28
7.2.14	<i>Automated Marking</i>	29
7.2.15	<i>Remote Access</i>	29
7.2.16	<i>Wireless Access Restrictions</i>	29
7.2.17	<i>Access Control for Portable and Mobile Devices</i>	29
7.2.18	<i>Personally Owned ICI Architectures</i>	30
7.3	AUDIT & ACCOUNTABILITY	30
7.3.1	<i>Audit and Accountability Policy and Procedures</i>	30
7.3.2	<i>Auditable Events</i>	30
7.3.3	<i>Content of Audit Records</i>	30
7.3.4	<i>Audit Storage Capacity</i>	30
7.3.5	<i>Audit Processing</i>	31
7.3.6	<i>Audit Monitoring, Analysis, and Reporting</i>	31
7.3.7	<i>Audit Reduction and Report Generation</i>	31
7.3.8	<i>Time Stamps</i>	31
7.3.9	<i>Protection of Audit Information</i>	31
7.3.10	<i>Audit Retention</i>	31
7.4	SYSTEM & COMMUNICATION PROTECTION	32
7.4.1	<i>System and Communications Protection Policy and Procedures</i>	32
7.4.2	<i>Application Partitioning</i>	32



Interoperable Communications Infrastructure

Security Policy

7.4.3	<i>Security Function Isolation</i>	32
7.4.4	<i>Information Remnants</i>	32
7.4.5	<i>Denial of Service</i>	32
7.4.6	<i>Resource Priority</i>	32
7.4.7	<i>Boundary Protection</i>	32
7.4.8	<i>Transmission Integrity</i>	33
7.4.9	<i>Transmission Confidentiality</i>	33
7.4.10	<i>Network Disconnect</i>	33
7.4.11	<i>Cryptographic Key Establishment and Management</i>	33
7.4.12	<i>Use of Validated Cryptography</i>	33
7.4.13	<i>Public Access Protections</i>	33
7.4.14	<i>Collaborative Computing</i>	34
7.4.15	<i>Public Key Infrastructure Certificates</i>	34
7.4.16	<i>Mobile Code</i>	34
7.4.17	<i>Voice Over Internet Protocol</i>	34
APPENDIX A: GLOSSARY OF TERMS, ROLES AND POSITIONS		35
APPENDIX A1: GLOSSARY OF TERMS		35
APPENDIX A2: GLOSSARY OF ROLES - ICI CENTRAL ROLES		41
APPENDIX A3: GLOSSARY OF ROLES - ICI PARTNER ROLES.....		43
APPENDIX B: REFERENCES		44
APPENDIX C: SAMPLE DOCUMENTATION		47
APPENDIX D: ICI SPECIFIC REFERENCES		47



Interoperable Communications Infrastructure

Security Policy

1 Purpose

The purpose of this Security Policy document is to set forth guidelines for the secure establishment and operation of the National Capital Region (NCR) Interoperable Communications Infrastructure (ICI). At a high-level, the NCR ICI applies to regional information systems, IT assets, applications, and networks. For specific details concerning the participants and composition of the ICI, refer to the document titled “*National Capital Region (NCR) Chief Information Officer’s (CIO) Interoperable Communications Infrastructure (ICI) Operations Plan (ICI Operations Plan)*.”

The intent of the controls recognized in this policy is to protect the confidentiality, integrity, and availability of the ICI and the information exchanged by the ICI with ICI Partners. This guidance shall also apply to regional systems connected to the ICI as practicable and applicable.

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

2 Objectives

The objective of this policy is to describe the security controls which apply to the design and implementation of the ICI and the day-to-day operations of the ICI Architecture, ICI regional information systems, applications, and networks in an effort to achieve its stated mission objectives.

This security policy discusses security-related requirements to facilitate a more consistent, comparable and repeatable approach for selecting and specifying security controls for the ICI 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 purposes of assessment and evaluation for determining security control effectiveness implemented in public safety systems, applications, and network services which connect to the ICI. The policies described in this document, and other security related documentation adopted by the ICI Chief Information Security Officer (CISO) Committee shall promote a dynamic, extensible catalog of security controls for the ICI to more efficiently meet the demands of changing requirements and technologies.

3 Scope

This policy applies to the National Capital Regional (NCR) Interoperable Communications Infrastructure (ICI). The NCR ICI consists of regional information systems, IT assets, applications, and networks, and all interconnected logical and physical components connected to the ICI. This consists of the personnel, technology, and operations supporting data



Interoperable Communications Infrastructure

Security Policy

exchanges, wireless and terrestrial networks between jurisdictions and/or mobile devices. This security policy does not address the security of components outside of the ICI domain.

Where circumstances prevent compliance with this policy, the ICI shall document exceptions to this security policy where necessary to facilitate ICI operations. The ICI CISO, with support from ICI Program Staff, shall work with regional systems/applications to document these exceptions following processes adopted by the Chief Information Security Officer (CISO) Committee (see section 5.1.1). More specifically, regional systems/applications shall work with ICI Program Staff to follow the adopted *ICI CISO Security Review Process* and *ICI Security Waiver or Exception Process* if the regional system/application is out of compliance with ICI security policy, standards, practices, or procedures.

As previously mentioned, the ICI Security Policy applies to regional information systems, applications, and networks. At the core of the ICI is the NCRNet – the demarcations have been defined, documented, and agreed to by the network managers of each interconnected jurisdiction. The ICI Security Policy applies to the NCRNet-maintained devices which interconnect the jurisdictional networks by way of a jurisdictionally-controlled firewall. Jurisdictional network security policy, whether documented or not, applies to this jurisdictionally controlled, NCRNet-connected firewall to allow access into or out of the jurisdictional network and to any subsequent systems connected directly or indirectly on the jurisdiction side of this firewall.

As per Figure 1 below, this boundary will be further documented and codified for all interconnected jurisdictions during the documentation of the risk assessment of the NCRNet. Boundaries will continue to be redefined as systems and applications are enabled in regionally-funded, non-jurisdictional data center facilities, or as regional applications and systems are operated from within a jurisdiction data center for regional use, or as changes occur to regional systems.

Concerning governance, the ICI Security Policy, and other security-related documentation adopted by the ICI CISO Committee, shall not conflict with information provided within the *ICI Operations Plan* pertaining to integration of governance and support functions for regional systems or applications being integrated into the operations of the ICI.



Interoperable Communications Infrastructure

Security Policy

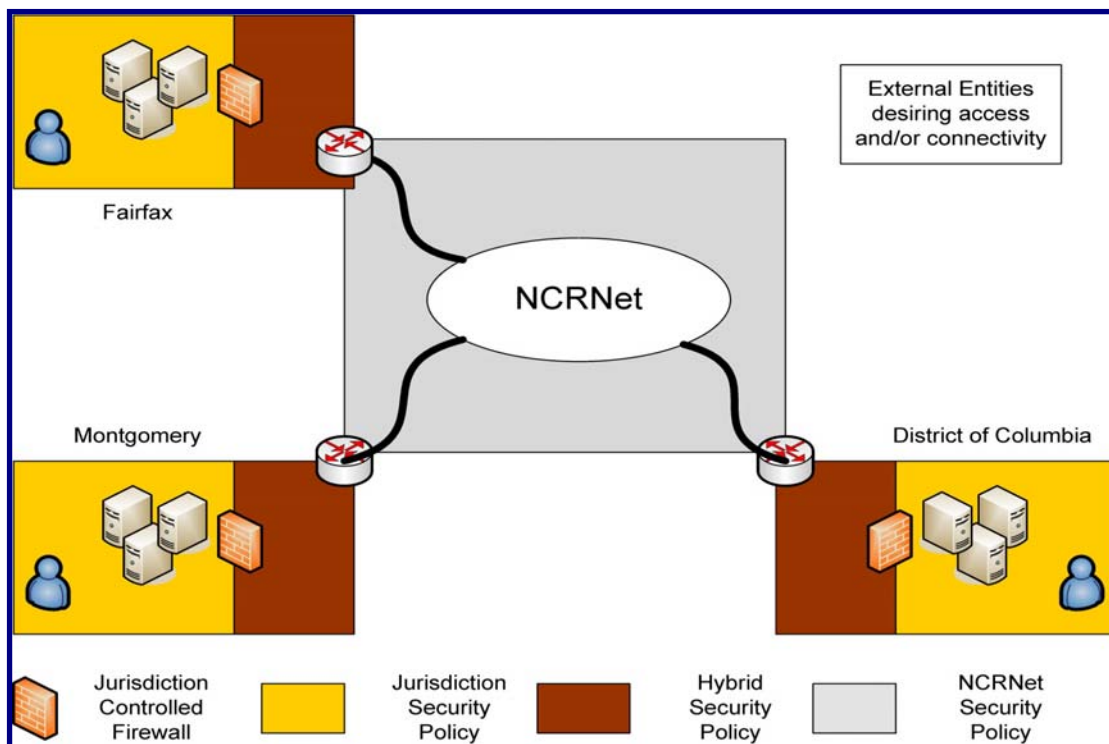


Figure 1- System Boundaries Determine Policy Authority which Governs Implementation of Controls

For regional systems/applications requiring utilization of the NCRNet for data connectivity, the regional Architectural Review Committee shall chair the evaluation and cutover of each regional application to interconnect with the NCRnet.

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

The Chief Information Officers (CIO) Subcommittee and Interoperability Council (IC) Subcommittee shall be responsible for reviewing instances when consensus between the ICI Partner and the ICI Organizations cannot be reached.

In summary, this policy, and other adopted CISO Committee security documentation shall be used by ICI Program Support personnel, and regional systems/applications, as a foundation for the purposes of assessment and evaluation of security controls. The policy shall be used for the NCR ICI, consisting of regional information systems, IT assets, applications, and networks, and all interconnected logical and physical components connected to the ICI.

4 Roles and Responsibilities

For the purpose of this document, the roles and responsibilities have been determined by a set of standard job responsibilities within the ICI, defined by all participating Jurisdictions, and



Interoperable Communications Infrastructure

Security Policy

relative to the ICI Architecture. The descriptions of each job responsibility shall not change; however, the titles are subject to change.

ICI roles and responsibilities are common across the *ICI Security Policy* (this document), the *Information Management Policy*, and the *IT Service Management Policy*. 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 ICI Personnel responsible for Risk Assessment (RA) controls for ICI systems/applications 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.

ICI Program Support, ICI CISO, and designated regional system/application personnel 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. All parties listed above shall work together to follow CISO Committee adopted processes for carrying out a risk assessment in the form of a survey between the ICI CISO, with assistance from ICI Program Support, and the partnering system/application. The partnering system/application will follow adopted policies for requesting relinquishment from controls that are deviated from, in the form of waiver(s) or exception(s). Details for these processes can be found in the following process documents:

- *CISO Committee Role in Processing an Application to Join the ICI*
- *ICI Security Waiver or Exception Process*

5.1.2 Security Categorization

The ICI CISO shall designate ICI Personnel within the ICI to review and approve the security categorizations.

The regional system/application, working with the ICI CISO and ICI Program Support Staff, 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 Security Survey Assessment for the system/application.

During the system security survey (risk) assessment, the ICI CISO and ICI Program Support Staff, working with the ICI Partner or other designated regional system/application personnel, shall determine the sensitivity or violability of the ICI Architecture to compromises in confidentiality, integrity, and availability of the information stored and processed by the system. The ICI CISO and ICI 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 ICI CISO, with ICI Program Staff support, shall conduct a security survey (risk) assessment of the regional system/application requesting to join the ICI network, or current



Interoperable Communications Infrastructure

Security Policy

system/applications that have undergone a major change to the ICI Architecture. ICI Architecture having been granted a security exception(s), shall be reevaluated after 1 year of the security exception(s) being issued. The ICI CISO, with ICI Program Support Staff, 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 ICI resources and information. A significant change to the system includes any change to the system architecture, operating system, or information processing capabilities.

The ICI Partner exchanging information with the ICI Architecture is strongly recommended to conduct a security survey assessment of the Information System or Application that shall be exchanging information with the ICI Architecture.

The ICI Program Support Staff shall conduct a security survey assessment on the interconnection between the ICI Architecture and the ICI Partner. This risk assessment shall be part of the formal Service Level Agreement (SLA) for the specific data exchange. The security assessment shall then be reviewed and validated by the ICI CISO, CISO Committee, and Architectural Review Committee (ARC) prior to submission to the CIO Committee.

The ICI CISO, with assistance from ICI Program Support Staff, shall identify and verify the levels of risk through conducting an assessment of the security controls and evaluate whether they provide adequate security for ICI Architecture and reduce the level of risk needed to obtain approval to join the ICI. The ICI CISO identifies additional control needs, evaluates cost-effective solutions, and the system owner assigns resources to implement corrective action (if necessary). The CISO Committee shall provide a recommendation to the CIO Committee for whether or not the Committee recommends the system/application for joining the ICI network. The CIO Committee shall then render a final decision to the system/application, per the Interoperable Communications Infrastructure (ICI) Operations Plan.

5.1.4 Vulnerability Assessment

Using appropriate vulnerability scanning tools and techniques, the regional system/application shall determine the need to scan for vulnerabilities within the ICI 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 ICI CISO shall update the list of vulnerabilities within the ICI Architecture at a specified frequency.

5.2 Planning

5.2.1 Security Planning Policy and Procedures

The ICI Personnel responsible for Planning (PL) controls for the ICI system/application 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.



Interoperable Communications Infrastructure

Security Policy

ICI Program Support, ICI CISO, and designated regional system/application personnel shall work together to document each security control in the form of a security assessment survey.

5.2.2 System Security Plan

The system or application owner shall work with designated ICI Program Staff to identify and document security controls and mechanisms either planned or implemented for the regional system or application. The system owners, working with the ICI CISO, and ICI Program Staff Support, shall develop, disseminate and implement a document of security controls and mechanisms implemented or planned for a regional system/application. The ICI CISO shall review and approve the documented security controls and determine any recommendations for remediation actions of planned or implemented security controls by the system/application.

The ICI CISO shall maintain documentation of security controls for the ICI Architecture for review by ICI Chief Information Officer as required.

5.2.3 Rules of Behavior

The ICI CISO shall establish and make readily available to all regional systems/applications a set of rules that describes their responsibilities and expected behavior when using the ICI.

Designated regional system/application personnel shall obtain signed acknowledgement documentation from ICI Users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the ICI Architecture. A sample Rules of Behavior can be found here:

<http://ncrportal.mwcog.org/sites/dehteam/Shared%20Documents/Enterprise%20Architecture/Security%20Domain/Security%20Policy/Rules%20of%20Behavior/Sample%20Rules%20of%20Behavior.htm>

5.3 System & Services Acquisition

5.3.1 System and Services Acquisition Policy and procedures

The ICI Personnel responsible for System and Services Acquisition (SA) controls for the ICI system/application 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.

5.3.2 Allocation of Resources

The regional system/application shall determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the ICI Architecture.



Interoperable Communications Infrastructure

Security Policy

5.3.3 Life Cycle Support

The regional system/application shall manage the ICI Architecture using a system development life cycle methodology that includes information security considerations.

5.3.4 Acquisitions

The regional system/application shall include security requirements and/or security specifications, either explicitly or by reference, in ICI Architecture acquisition contracts based on an assessment of risk.

The systems and services provided by contractors to the ICI Architecture shall be governed by the security requirements and/or specifications identified by the regional system/application. 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 regional system/application shall ensure that adequate documentation for the ICI 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 ICI Architecture with sufficient detail to permit analysis and testing of the controls.

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

5.3.6 Software Usage Restrictions

All ICI Users of the ICI Architecture shall comply with software usage restrictions. The ICI 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 regional system/application shall enforce explicit rules governing the downloading and installation of software by ICI Users.

5.3.8 Security Design Principles

The regional system/application shall design and implement the ICI Architecture using sound security engineering principles as defined by the National Institute of Standards and Technology, SANS Institute, and other industry best practices provided by the CISO Committee.



Interoperable Communications Infrastructure

Security Policy

5.3.9 Outsourced Services

The regional system/application shall ensure that third-party providers of ICI Architecture services and ICI 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 methods such as periodic inquiries, through continuous monitoring.

6 Operational Security Policy

6.1 Personnel Security

6.1.1 Personnel Security Policy and Procedures

The ICI Personnel responsible for Personnel Security (PS) controls within the partnering ICI system/application 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 ICI CISO, with ICI Program Staff support, shall facilitate the communication process with designated regional system/application personnel on matters relevant to personnel security.

The ICI CISO, with ICI Program Staff support, shall be responsible for ensuring that the ICI staff and contractor position is designated at the appropriate level of position sensitivity and/or risk. The ICI CISO 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 ICI CISO shall assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The ICI CISO shall also review and revise position risk designations at specified frequency or every three years.

Where feasible, the regional system/application shall separate sensitive duties to preclude any one individual from gaining the opportunity to adversely affect the ICI Architecture. The ICI CISO shall ensure that the regional system/application has defined procedural checks and balances for personnel security. The ICI CISO shall ensure enforceability of these controls so that accountability is established and security violations are detectable.

6.1.3 Personnel Screening

The regional system/application shall screen individuals requiring access to organizational information before authorizing access.



Interoperable Communications Infrastructure

Security Policy

Foreign nationals shall not be granted access to or perform critical sensitive duties on the ICI Architecture, unless express permission is provided by the regional system owner or application owner.

The ICI CISO shall ensure that a risk-based, cost-effective approach is followed to determine the risk of harm to the ICI 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 ICI system/application administrator shall terminate access to the ICI Architecture.

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

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

6.1.5 Personnel Transfer

The ICI CISO shall review ICI Architecture facility access authorizations when individuals are reassigned or transferred to other positions within the ICI 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 ICI CISO and designated regional system/application personnel shall ensure that the ICI 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 ICI User of the ICI 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 ICI Architecture, the System Administrator shall ensure that each agreement is signed and dated.

6.1.7 Third-Party Personnel Security

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



Interoperable Communications Infrastructure

Security Policy

The ICI CISO shall monitor provider compliance to ensure adequate security.

6.1.8 Personnel Sanctions

The ICI CISO shall enforce formal sanctions, for personnel failing to comply with established ICI Architecture security policies and procedures.

6.2 Physical & Environmental Protection

6.2.1 Physical and Environmental Protection Policy and Procedures

The ICI Personnel responsible for Physical and Environment Protection (PE) controls within the partnering ICI system/application 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 ICI CISO shall develop and keep current lists of personnel with authorized access to facilities within the ICI 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 ICI Partner shall review and approve the access list and authorization credentials at a specified frequency, at least annually.

6.2.3 Physical Access Control

The ICI CISO shall designate personnel to control all physical access points (including designated entry/exit points) to facilities within the ICI 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

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

6.2.5 Monitoring Physical Access

The regional system/application shall designate an official to monitor physical access to the ICI Architecture to detect and respond to incidents. The ICI designated official 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.



Interoperable Communications Infrastructure

Security Policy

6.2.6 Visitor Control

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

6.2.7 Access Logs

The ICI CISO and the ICI Partner shall maintain a visitor access log to facilities within the ICI 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 ICI CISO and the ICI Partner shall review the access logs at a specified frequency after closeout.

The ICI Partner shall employ automated mechanisms to facilitate the maintenance and review of access logs.

6.2.8 Power Equipment and Power Cabling

The ICI CISO and the ICI Partner shall ensure the protection of power equipment and power cabling for the ICI Architecture from damage and destruction.

6.2.9 Emergency Shutoff

For specific locations within a facility containing concentrations of ICI Architecture resources (e.g., data centers, server rooms, mainframe rooms), the ICI CISO and the ICI 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 ICI CISO and the ICI Partner shall ensure short-term uninterruptible power supply to facilitate an orderly shutdown of the ICI Architecture in the event of a primary power source loss. In addition, the ICI CISO and ICI Partner shall ensure a long-term alternate power supply for the ICI 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 ICI CISO and the ICI Partner shall be notified immediately upon loss of system use.



Interoperable Communications Infrastructure

Security Policy

6.2.11 Fire Protection

The ICI CISO and the ICI 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 ICI Architecture.

6.2.12 Temperature and Humidity Controls

The ICI CISO and ICI Partner shall ensure facilities containing ICI Architecture equipment are monitored and maintained within acceptable levels of temperature and humidity.

6.2.13 Water Damage Protection

The ICI CISO and the ICI Partner shall ensure all facilities containing ICI 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 ICI CISO and the ICI Partner shall control ICI 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 ICI CISO and the ICI Partner shall employ appropriate ICI Architecture security controls at alternate work sites.

6.3 Contingency Planning

6.3.1 Contingency Planning Policy and Procedures

The ICI Personnel responsible for Contingency Planning (CP) controls within the partnering ICI system/application 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 ICI Partner 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.



Interoperable Communications Infrastructure

Security Policy

The ICI CISO shall review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

The ICI Partner shall designate personnel to coordinate contingency plan development within the organization.

6.3.3 Contingency Training

The ICI Partner shall ensure all personnel are adequately trained in their contingency roles and responsibilities with respect to the ICI Architecture. The ICI Partner 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.

6.3.4 Contingency Plan Testing

The ICI regional system/application owner shall designate personnel to test the contingency plan at a specified frequency, at least annually using specified tests and exercises to determine the plan's effectiveness and the ICI Architecture's readiness to execute the plan. The ICI system/application 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 ICI CISO shall then review the contingency plan test results and initiate corrective actions.

The ICI system/application shall designate personnel to coordinate contingency plan testing within the organization.

6.3.5 Alternate Storage Site

The ICI CISO and ICI Partner shall identify an alternate storage site and initiate necessary agreements to permit the storage of ICI 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 ICI Partner 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 ICI Partner shall identify any need for an alternate processing site and initiate necessary agreements to permit the resumption of ICI 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



Interoperable Communications Infrastructure

Security Policy

alternate processing site shall be geographically separated from the primary processing site so as not to be susceptible to the same hazards.

The ICI Partner 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 ICI Partner shall identify any need for primary and alternate telecommunications services to support the ICI 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 service agreements should contain priority-of-service provisions in accordance with the organization's availability requirements.

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

The ICI Partner shall ensure that adequate contingency plans for primary and alternate telecommunications service providers (if applicable) are instituted.

6.3.8 ICI Architecture Backup

The ICI CISO and the ICI Partner shall ensure the archival of all data and metadata under their cognizant authority.

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

The ICI CISO and the ICI Partner shall test backup information at specified frequency to ensure media reliability and information integrity.

The ICI CISO and the ICI Partner shall selectively use backup information in the restoration of ICI Architecture functions as part of contingency plan testing.

The ICI CISO and the ICI Partner shall ensure backup copies of the operating system and other critical ICI 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 ICI CISO.

6.3.9 ICI Architecture Recovery and Reconstitution

The ICI CISO and the ICI Partner shall employ mechanisms with supporting procedures to allow the ICI Architecture to be recovered and reconstituted to the system's original state after



Interoperable Communications Infrastructure

Security Policy

a disruption or failure. Full recovery and reconstitution of the ICI Architecture shall be included as part of contingency plan testing.

6.4 Configuration Management

6.4.1 Configuration Management Policy and Procedures

The ICI Personnel responsible for Configuration Management (CM) controls within the partnering ICI system/application 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 ICI CISO and partnering ICI system/application shall identify configuration baselines for the item to be configured -- what the item is (e.g., system specifications, system or program documentation, 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. The identified CM baselines shall adhere to the Configuration Management guidelines set forth in the Regional Information Technology Service Management (ITSM) policy.

During configuration change control the partnering ICI system/application shall provide a request for recommended changes to the ICI CISO in writing for approval. The system/application shall also ensure that approved changes are tested before implementation.

The regional system/application shall track all approved changes to the ICI Architecture and maintain documentation associated with authorized changes.

6.4.2 Baseline Configuration

The regional system/application owner, shall develop, document, and maintain a current, baseline configuration of the ICI Architecture and an inventory of the system's constituent components, update the baseline configuration as an integral part of ICI 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 ICI Partner shall document and control changes to the ICI Architecture. The ICI CISO shall approve ICI Architecture changes in accordance with organizational policies and procedures.

The ICI Partner shall employ automated mechanisms to: (i) document proposed changes to the ICI 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 ICI Architecture.



Interoperable Communications Infrastructure

Security Policy

6.4.4 Monitoring Configuration Changes

The ICI Partner shall monitor changes to the ICI Architecture and conduct security impact analyses to determine the effects of the changes.

6.4.5 Access Restrictions for Change

The ICI Partner shall enforce access restrictions associated with changes to the ICI Architecture. The Partner shall also employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

6.4.6 Configuration Settings

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

6.4.7 Least Functionality

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

The ICI CISO shall review the ICI 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 ICI Personnel responsible for Maintenance (MA) controls within the partnering ICI system/application shall develop, disseminate, and periodically review/update: (i) a formal, documented, ICI Architecture maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the ICI Architecture maintenance policy and associated system maintenance controls.

6.5.2 Periodic Maintenance

The regional system/application shall schedule, perform, and document routine preventative and regular maintenance on the components of the ICI Architecture in accordance with manufacturer or vendor specifications and/or ICI Architecture requirements. In addition, the regional system/application shall maintain a log for the ICI 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).



Interoperable Communications Infrastructure

Security Policy

The regional system/application 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 regional system/application shall approve, control, and monitor the use of ICI Architecture maintenance tools and maintain the tools on an ongoing basis.

The regional system/application shall ensure the inspection of all ICI Architecture maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

The regional system/application shall ensure that all ICI 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 ICI Architecture.

The regional system/application 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 ICI Architecture or is destroyed, unless an appropriate ICI Architecture official explicitly authorizes an exception.

6.5.4 Remote Maintenance

The regional system/application 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 ICI Architecture.

The regional system/application shall ensure that remote diagnostic or maintenance services within the ICI Architecture implements the same level of security as that implemented on the ICI Architecture being serviced.

6.5.5 Maintenance Personnel

The ICI CISO shall maintain a list of personnel authorized to perform maintenance on the ICI Architecture.

The ICI CISO shall ensure that only authorized personnel perform maintenance on the ICI Architecture and those personnel have appropriate access authorizations.

6.5.6 Timely Maintenance

The ICI CISO shall obtain maintenance support and spare parts for specified list of key ICI Architecture components within specified time period of failure.



Interoperable Communications Infrastructure

Security Policy

6.6 System & Information Integrity

6.6.1 System and Information Integrity Policy and Procedures

The ICI Personnel responsible for System and Information Integrity (SI) controls within the partnering ICI system/application 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 regional system/application, working with the CISO shall identify, report, and correct ICI Architecture flaws.

6.6.3 Malicious Code Protection

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

The ICI Partner shall employ virus protection mechanisms at critical ICI 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 ICI Partner shall also implement malicious code protection that includes a capability for automatic updates and ensure that the system shall centrally manage virus protection mechanisms and automatically update virus protection mechanisms.

6.6.4 Intrusion Detection Tools and Techniques

The ICI Partner shall employ tools and techniques to monitor events on the ICI Architecture, detect attacks, and provide identification of unauthorized use of the system.

6.6.5 Security Alerts and Advisories

The ICI CISO shall employ automated mechanisms to receive ICI Architecture security alerts/advisories on a regular basis.

In the case of an alert, the ICI CISO shall issue alerts/advisories to the regional partnering system(s) or application(s), to 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 ICI Partners.



Interoperable Communications Infrastructure

Security Policy

6.6.6 Security Functionality Verification

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

The ICI CISO shall enforce automated mechanisms to provide notification of failed security tests.

6.6.7 Software and Information Integrity

The regional system/application shall ensure detection and protection against unauthorized changes to software and information.

The regional system/application shall employ integrity verification applications in the ICI Architecture to monitor for information tampering, errors, and omissions.

6.6.8 Spam and Spyware Protection

The regional system/application shall ensure the implementation of spam and spyware protection that is centrally managed.

The regional system/application shall employ spam and spyware protection mechanisms at critical ICI 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 regional system/application shall restrict the information input to the ICI Architecture to authorized personnel only.

6.6.10 Information Output Handling and Retention

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

6.6.11 Error Handling

The regional system/application shall ensure that error conditions are identified and handled in an expeditious manner.



Interoperable Communications Infrastructure

Security Policy

6.6.12 Information Output Handling and Retention

The ICI Partner shall ensure the proper handling and output, of ICI Architecture information.

The ICI Partner shall ensure the proper retention of information under their authority.

6.7 Media Protection

6.7.1 Media Protection Policy and Procedures

The ICI Personnel responsible for Media Protection (MP) controls within the partnering ICI system/application 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 ICI CISO and ICI Partner shall provide the ICI Architecture with a comprehensive outline that clearly defines the level of access granted to ICI Users based on roles and responsibilities as described in this ICI Security Policy.

The ICI CISO shall ensure that only authorized ICI users have access to information in printed form or on digital media removed from the ICI Architecture.

Unless guard stations control access to media storage areas, the ICI Partner 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 ICI CISO and ICI Partner shall affix external labels to electronic files, hard copy printouts, and removable media (diskettes and CD-ROMs) containing system/application data.

Also, the ICI CISO and ICI Partner shall affix external labels to removable information storage media and ICI Architecture output indicating the distribution limitations and handling caveats of the information.

6.7.4 Media Storage

The ICI CISO and the ICI Partner shall establish methods (if any) for ensuring that ICI Architecture media storage is physically controlled and securely stored, both paper and digital.



Interoperable Communications Infrastructure

Security Policy

6.7.5 Media Transport

The ICI CISO and the ICI Partner shall control ICI 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 CISO and the ICI Partner shall ensure the proper sanitization of media, where appropriated.

6.7.7 Media Destruction and Disposal

The ICI CISO and the ICI Partner shall sanitize or destroy ICI 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 ICI Personnel responsible for Incident Response (IR) controls within the partnering ICI system/application 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 ICI CISO and the ICI Partner shall establish a method of support (if needed) to effectively monitor, respond, report, and prevent incidents occurring during exchanges with the ICI Architecture. This includes the communication of incident information to ICI Partners by ICI personnel.

The regional system/application users shall report security incidents, suspected or otherwise, to the system/application owner. In turn, the system/application owner should provide all relevant security to the ICI CISO. The ICI CISO shall communicate incident information to impacted ICI Partners.

The regional system/application 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.

6.8.2 Incident Response Training

The regional system/application shall ensure adequate training for personnel in their incident response roles and responsibilities with respect to the ICI Architecture and provide refresher training at specified frequency, at least annually.



Interoperable Communications Infrastructure

Security Policy

The regional system/application shall ensure that simulated events are incorporated into ICI Architecture incident response training to facilitate effective response by personnel in crisis situations.

6.8.3 Incident Response Testing

The regional system/application shall test the ICI 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 regional system/application shall employ automated mechanisms to more thoroughly and effectively test the incident response capability.

6.8.4 Incident Handling

The regional system/application shall ensure the implementation of an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

The regional system/application shall also employ automated mechanisms to support the incident handling process.

6.8.5 Incident Monitoring

The regional system/application shall track and document ICI 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

ICI Users of the ICI Architecture shall report incident information to the ICI CISO. The ICI CISO shall accept incident information from ICI Partners.

The regional system/application shall employ automated mechanisms to assist in the reporting of security incidents. The ICI CISO shall employ available mechanisms, automated or otherwise, to report incident information to impacted ICI Partners.

The ICI CISO 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).

6.8.7 Incident Response Assistance

The regional system/application shall ensure the availability of an incident response support resource that offers advice and assistance to Users of the ICI Architecture for the handling and



Interoperable Communications Infrastructure

Security Policy

reporting of security incidents. The support resource shall be an integral part of the organization's incident response capability.

The regional system/application 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 ICI Personnel responsible for Security Awareness Training (AT) controls within the partnering ICI system/application 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 regional system/application shall ensure all ICI staff and contractors are exposed to basic ICI Architecture security awareness materials before authorizing access to the system and on an annual basis thereafter.

6.9.3 Security Training

The regional system/application shall identify personnel with significant ICI Architecture security roles and responsibilities and then provide documentation of those roles and responsibilities.

The ICI CISO shall ensure appropriate ICI Architecture security training is available to ICI Users before authorizing access to the system and periodically thereafter.

6.9.4 Security Training Records

The regional system/application shall document and monitor individual ICI Architecture security training activities including basic security awareness training and specific ICI Architecture security training.



7 Technical Security Policy

7.1 Identification & Authentication

7.1.1 Identification and Authentication Policy and Procedures

The ICI Personnel responsible for Identification and Authentication (IA) controls within the partnering ICI system/application 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 ICI shall ensure unique identification and authentication of ICI Users (or processes acting on behalf of users) and that each employ multifactor authentication. The ICI CISO shall ensure the ICI Architecture can support identification and authentication needs set forth in Service Level Agreements.

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

7.1.3 Device Identification and Authentication

The ICI 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 ICI Partner information systems for the purposes of data exchange.

7.1.4 Identifier Management

The ICI 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 ICI shall ensure the management of ICI 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 ICI Architecture installation.



Interoperable Communications Infrastructure

Security Policy

7.1.6 Authentication Feedback

The ICI shall ensure ICI 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 ICI shall ensure the ICI 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 ICI Personnel responsible for Access Control (AC) security controls within the partnering ICI system/application 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 regional system/application 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 ICI Architecture service.

The regional system/application shall authorize all special access accounts required for audit, software development, software installation, or other defined need.

The regional system/application 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 regional system/application, the System Administrator shall manage ICI Architecture accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

The ICI regional system/application 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 regional system/application shall employ automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.



Interoperable Communications Infrastructure

Security Policy

The regional system/application shall review ICI Architecture accounts periodically and employ automated mechanisms to support the management of ICI Architecture accounts.

7.2.3 Access Enforcement

The regional system/application shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

The regional system/application 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 regional system/application shall ensure the cryptographic devices employ NIST FIPS 140-2 compliance for encryption.

7.2.4 Information Flow Enforcement

The regional system/application shall enforce assigned authorizations, as authorized by the ICI CISO, for controlling the flow of information within the ICI Architecture and between data exchanges in accordance with applicable policy.

7.2.5 Separation of Duties

The regional system/application shall enforce separation of duties through assigned access authorizations. Separation of duties shall occur between regional system/application, ICI System Administrator, and the ICI CISO.

7.2.6 Least Privilege

The regional system/application shall enforce an established set of rights/privileges or accesses needed by ICI Users (or processes acting on behalf of users) for the performance of specified tasks.

7.2.7 Unsuccessful Login Attempts

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

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

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



Interoperable Communications Infrastructure

Security Policy

7.2.8 System Use Notification

The regional system/application shall ensure the display an approved, system use notification message before granting system access informing potential ICI and ICI Partner Users: (i) that the user is accessing a the ICI; (ii) that system usage may be monitored, recorded, and subject to 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 regional system/application 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 ICI Architecture.

7.2.9 Concurrent Session Lock

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

7.2.10 Session Lock

The ICI 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 ICI System Administrator shall ensure automatic termination of a session after a specified period of inactivity.

7.2.12 Supervision and Review – Access Control

The ICI CISO shall ensure the supervision and review the activities of ICI and ICI Partner Users with respect to the enforcement and usage of ICI Architecture access controls.

The ICI CISO shall ensure the implementation of automated mechanisms to facilitate the review of ICI and ICI Partner User activities.

7.2.13 Permitted Actions without Identification and Authentication

The regional system/application shall identify specific user actions that can be performed on the ICI Architecture without identification or authentication and permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.



Interoperable Communications Infrastructure

Security Policy

7.2.14 Automated Marking

The ICI Partner shall ensure marked output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

7.2.15 Remote Access

The regional system/application shall document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the ICI Architecture including remote access for privileged functions.

The regional system/application shall authorize each remote access method and authorize only the necessary ICI Users for each access method.

The ICI CISO 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 ICI 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 regional system/application, working in conjunction with the ICI CISO, shall establish usage restrictions and implementation guidance for wireless technologies.

The regional system/application, working in conjunction with the ICI CISO, shall document, monitor, and control wireless access to the ICI Architecture.

The regional system/application, working in conjunction with the ICI CISO, shall ensure the use of authentication and encryption to protect wireless access to the ICI Architecture.

The ICI support personnel, working in conjunction with the ICI CISO, shall employ security controls to restrict the ability to connect to more than one wireless data network.

The ICI CIO Committee shall review all situations involving access restrictions for wireless technologies, where a consensus between the ICI CISO and the Jurisdictional systems or applications cannot be reached.

7.2.17 Access Control for Portable and Mobile Devices

The regional system/application shall establish usage restrictions and implementation guidance for portable and mobile devices and document, monitor, and control device access to the ICI Architecture.



Interoperable Communications Infrastructure

Security Policy

The ICI CISO shall employ removable hard drives or cryptography to protect information residing on portable and mobile devices.

The ICI CISO shall employ logical device locking mechanisms inherent to a portable or mobile device to restrict access to the device.

7.2.18 Personally Owned ICI Architectures

The regional system/application shall restrict the use of personally owned information systems for official ICI Architecture business involving the processing, storage, or transmission of data contained within the ICI Architecture.

7.3 Audit & Accountability

7.3.1 Audit and Accountability Policy and Procedures

The ICI Personnel responsible for Audit and Accountability (AU) controls within the partnering ICI system/application 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 ICI CISO shall ensure the generation of audit records for the specified events.

7.3.3 Content of Audit Records

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

The regional system/application 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 ICI CISO shall ensure the allocation of sufficient audit record storage capacity and configure auditing to prevent such capacity being exceeded.



Interoperable Communications Infrastructure

Security Policy

7.3.5 Audit Processing

The ICI CISO shall ensure the ICI Architecture has a mechanism for alerting the ICI System Administrator and regional system/application, in the event of an audit failure or audit storage capacity being reached. In such an event the ICI CISO shall take specified actions to ensure the complete recovery of audit records.

The ICI CISO shall ensure the ICI 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 regional system/application 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.

The regional system/application shall ensure the ICI 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 ICI CISO shall ensure the ICI 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 ICI Architectural Review Committee (ARC) and CISO Committee shall ensure that ICI Architecture provides time stamps for use in audit record generation.

7.3.9 Protection of Audit Information

The ICI Architectural Review Committee (ARC) and CISO Committee shall ensure that the ICI Architecture provides adequate protection of audit information and audit tools from unauthorized access, modification, and deletion.

7.3.10 Audit Retention

The ICI CISO 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.



Interoperable Communications Infrastructure

Security Policy

7.4 System & Communication Protection

7.4.1 System and Communications Protection Policy and Procedures

The ICI Personnel responsible for System and Communications Protection (SC) controls within the partnering ICI system/application 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 ICI CISO shall ensure the separation of user functionality (including user interface services) from ICI Architecture management functionality.

7.4.3 Security Function Isolation

The ICI CISO shall ensure that the ICI Architecture isolates security functions from non-security functions.

7.4.4 Information Remnants

The ICI CISO shall ensure that the ICI Architecture prevents unauthorized and unintended information transfer via shared system resources.

7.4.5 Denial of Service

The ICI CISO shall ensure the ICI Architecture protects against or limit the effects of specified types of denial of service attacks.

The ICI CISO shall ensure the ICI 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 ICI CISO shall ensure the ICI Architecture limits the use of resources by priority.

The ICI CISO shall implement and maintain procedures that ensure ICI 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 ICI CISO shall ensure the ICI Architecture monitors and controls communications at the external boundary of the ICI Architecture and at key internal boundaries within the system.



Interoperable Communications Infrastructure

Security Policy

The ICI CISO shall ensure the ICI Architecture physically allocates publicly accessible ICI 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 ICI CISO shall ensure the ICI Architecture uses logical security controls to protect ICI Architecture components from network disruptions.

7.4.8 Transmission Integrity

The ICI ISO shall ensure ICI 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 ICI CISO shall ensure the ICI Architecture protects the confidentiality of transmitted information and employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

7.4.10 Network Disconnect

The ICI CISO shall ensure the ICI 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 ICI CISO shall ensure the ICI 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 ICI CISO shall ensure the ICI Architecture performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation. The ICI CISO shall work with the regional system/application to assess the level of risk associated with the system/application, and determine if validated cryptography shall be used.

7.4.13 Public Access Protections

The ICI CISO shall ensure the ICI Architecture shall protect the integrity of the information and applications within public service zones.



Interoperable Communications Infrastructure

Security Policy

7.4.14 Collaborative Computing

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

7.4.15 Public Key Infrastructure Certificates

The ICI CISO shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the ICI Architecture.

7.4.16 Mobile Code

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

The ICI CISO, working with the regional system/application, shall document, monitor, and control the use of mobile code within the ICI Architecture.

7.4.17 Voice Over Internet Protocol

The ICI CISO, working in conjunction with the regional system/application, shall establish usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the ICI Architecture if used maliciously.

The ICI ARC and CISO Committee shall review all situations involving VOIP, where a consensus between the ICI CISO and the regional system/application cannot be reached.

The regional system/application shall document, monitor, and control the use of VOIP within the ICI Architecture.

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 ICI, information from jurisdictions determined to be accessed or updated frequently shall be cached on the ICI 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 an ICI 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).



Interoperable Communications Infrastructure

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 shall 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 the ICI, 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 ICI; and provides timely notification to subscribers when the integrity of information is in question.

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>.



Interoperable Communications Infrastructure

Security Policy

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

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

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

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

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

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

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

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

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

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

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



Interoperable Communications Infrastructure

Security Policy

information sharing is accomplished both horizontally across the government and vertically among federal, state and local governments, private sector and citizens as outlined in the President's National Strategy for Homeland Security.

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

Information Management includes the use of a document and hierarchical information management system. The process ensures that the right information is stored in the appropriate media, with the right level of access and speed of retrieval. Information Management domain supports the following objectives from the NCR ICI 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.



Interoperable Communications Infrastructure

Security Policy

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

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

ICI Architecture consists of the infrastructure, applications, information and services deployed to achieve the ICI mission.

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

ICI Demarcation The point within the ICI 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 Interoperability Program intended to offer optical, high speed, resilient networking capabilities to ICI member jurisdictions.

ICI Partner Data ICI Partner Data is defined as the data that is owned by the ICI Partner. There shall be a single primary owner of this data.

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

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

ICI Operational Environment The organization, human resources and operational resources of the ICI.

ICI Service is a technical Web service that can be provided or consumed according to standard Web service protocols (i.e., SOAP, WSDL, UDDI). ICI Web Services facilitate data exchange and system interoperability by providing common system routines that can be used by various ICI 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 shall 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.



Interoperable Communications Infrastructure

Security Policy

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

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

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

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

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

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

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

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

Service Delivery is 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, ICI Architecture, and the service recipient, the ICI 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 shall 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 - ICI Central Roles

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

The **ICI Chief Information Officer (CIO)** shall ensure organizational compliance with laws and regulations. Establish and adopt ICI strategies. Ensure their respective ICI 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 **ICI Chief Information Security Officer (CISO)** shall possess professional qualifications, including training and experience, required to administer the information security functions of the ICI Architecture. The ICI SAISO is primarily responsible for implementing existing and converging security policies as defined by national, state, local government, and organizational policies. The ICI CISO reports to both the ICI CISO Committee, and CIO Committee on matters relative to the security operations of the ICI Architecture. The ICI CISO is also responsible for ensuring the appropriate operational security posture is maintained for the ICI Architecture and shall serve as the principal advisor to the CISO Committee on all matters (technical and otherwise) involving the security of the system. The ICI CISO shall be responsible for monitoring and providing reports on IT security program matters to the ICI CISO and CIO Committees.

The **ICI System/Application Owner** is responsible for the overall procurement, development, integration, modification, or operation and maintenance of the ICI Architecture; development and maintenance of the system security documentation; and deployment and operation, according to the agreed-upon security requirements. The ICI System/Application Owner shall maintain responsibility for determining who has access to the ICI 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 **ICI Program Support Staff** is responsible for providing support for all activities related to integration of partnering systems or applications to joining the ICI. The Program Support Staff is also responsible for coordinating security efforts with the system/application, ICI CISO, CISO Committee, and any other participating parties as deemed appropriate by the ICI CISO. The Program Support Staff will work with the system/application designated personnel to conduct a risk assessment in the form of a security survey, and carrying out activities set forth by the CIO Committee, CISO Committee, and ARC.

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



Interoperable Communications Infrastructure

Security Policy

The **ICI User** is any individual or automated application or process that is authorized access to the resource by the ICI Regional System/Application, in accordance with the practices and procedures associated with the ICI. All ICI Users have the responsibility to comply with law, regulation, policy, standards, practices, and procedural controls in order to protect Information resources and authorized use of data within their custody. ICI 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 - ICI Partner Roles

The following terms and descriptions represent roles and responsibilities applicable to ICI Partners such as ICI Jurisdictional Personnel, ICI Partner systems and services.

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

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

The **ICI Partner User** is any individual or automated application or process that is authorized access to the resource by the ICI System/Application. All ICI 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. ICI Partner Users of data may be further decomposed to establish a role-based access structure for more granular control of access to applications and/or data.

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

ICI Regional System/Application is a system or application which fulfills specific business functions for the National Capital Region (NCR) ICI and directly benefits specific users of the application or system.

ICI User Workstation is a computing asset operated by an end user to interact with local and regional applications and servers, and ICI applications and servers.



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.



Interoperable Communications Infrastructure

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.



Interoperable Communications Infrastructure

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:

- ❖ Risk Assessment Sample

Appendix D: ICI Specific References

Samples of the following documents are available upon request:

- ❖ Application over NCR ICI Request Form
- ❖ CISO Committee Security Review Process for Applications Joining ICI
- ❖ Application Survey Initiation Form
- ❖ Survey Assessment Spreadsheet
- ❖ Application Requester Checklist
- ❖ Security Waiver or Exception Procedures
- ❖ Security Waiver or Exception Process
- ❖ Request for Security Waiver or Exception Form
- ❖ Recommendation for Security Waiver or Exception Form