RITA Intelligent Transportation Systems Joint Program Office

Core System Requirements Specification (SyRS)

www.its.dot.gov/index.htm

Revision A — June 13, 2011

U.S. Department of Transportation

Research and Innovative Technology Administration

Produced by Lockheed Martin
ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD MM YYYY)	2. REPORT TYPE	3. DATES COVERED
13 06 2011	(Draft Specification)	Month YYYY – Month YYYY

4. TITLE AND SUBTITLE
Core System Requirements Specification (SyRS) Revision A

5a. CONTRACT NUMBER
GS-23F-0150S
5b. GRANT NUMBER
Xxxx
5c. PROGRAM ELEMENT NUMBER
Xxxx
5d. PROJECT NUMBER
DTFH61-10-F-00045
5e. TASK NUMBER
Xxxx
5f. WORK UNIT NUMBER
Xxxx

6. AUTHOR(S)
Core System Engineering Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lockheed Martin
9500 Godwin Drive
Manassas, VA 20110

8. PERFORMING ORGANIZATION REPORT NUMBER
11-USDOTSE-LMDM-00023

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Department of Transportation
Research and Innovative Technology Administration
ITS Joint Program Office
1200 New Jersey Ave., S.E.
Washington D.C. 20590

10. SPONSORING/MONITOR'S ACRONYM(S)
Xxxx

11. SPONSORING/MONITOR'S REPORT NUMBER(S)
Xxxx

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

12b. DISTRIBUTION CODE
Xxxx

13. SUPPLEMENTARY NOTES
Xxxx

14. ABSTRACT (Maximum 200 words)
Xxxx

15. SUBJECT TERMS
Xxxx

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	None	Xxxx	Walt Fehr
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER: (202) 366-0278

CHANGE LOG

Revision	*Change Summary*	*Author*	*Date*
-	Initial Release	Lockheed Martin	4/18/2011
A	Disposition of both Customer comments and Walkthrough comments incorporated in this revision.	Lockheed Martin	6/13/2011

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Scope

1.1 Identification

This document is the System Requirements Specification (SyRS) of the Core System for the United States Department of Transportation's (USDOT) *connected vehicle* program. This is document number: 11-USDOTSE-LMDM-00023.

1.2 Document Overview

The USDOT initiated this Systems Engineering (SE) project to define the ConOps, requirements, and architecture for a system that will enable safety, mobility, and environmental applications in an environment where vehicles and personal mobile devices are connected wirelessly, hereafter referred to as the *connected vehicle* environment.

The ConOps is a prerequisite to this document and is recommended reading prior to the SyRS. The ConOps describes the characteristics of the Core System from the system user's viewpoints. The SyRS builds upon those concepts, particularly the User Needs, to document the required functionality, performance, interfaces, and other required characteristics for the Core System.

The structure of this SyRS document is based on Institute of Electrical and Electronics Engineers (IEEE) Standard 1233-1998 IEEE Guide for Developing System Requirements Specifications and Federal Highway Administration's (FHWA) System Engineering Guidebook (SEGB) that adapted IEEE-1233.

The SyRS document consists of the following sections:

- Section 1 provides an overview of the Core System and an introduction to this SyRS document.
- Section 2 lists the documents used as background information or as a source of requirements.
- Section 3 provides the requirements for the Core System. They are organized by the level, either System or one of the 8 subsystems, and then by type of requirement.
    - Section 3.1: System Requirements
        - Section 3.1.1: System Functional Requirements
        - Section 3.1.2: System Performance Requirements
        - Section 3.1.3: System Interface Requirements
        - Section 3.1.4: System Data Requirements
        - Section 3.1.5: Non-Functional System Requirements
        - Section 3.1.6: Enabling Requirements
        - Section 3.1.7: Constraints

- Section 3.2: Subsystem Requirements
  - Section 3.2.1: Core2Core Subsystem Requirements
  - Section 3.2.2: Data Distribution Subsystem Requirements
  - Section 3.2.3: Misbehavior Management Subsystem Requirements
  - Section 3.2.4: Network Services Subsystem Requirements
  - Section 3.2.5: Service Monitor Subsystem Requirements
  - Section 3.2.6: Time Subsystem Requirements
  - Section 3.2.7: User Permissions Subsystem Requirements
  - Section 3.2.8: User Security Subsystem Requirements

The subsystem requirements sections each include the functional, performance, interface, and data requirements for that subsystem.

- Section 4 lists the Verification Method of each requirement from Section 3.
- Section 5 provides a listing of Supporting Documentation.
- Section 6 provides the Traceability Matrices tracing each requirement to the User Needs and vice versa.
- Section 7 contains a Glossary of terms and a listing of abbreviations and acronyms.
- Section 8 contains a table of Metric to English measurement conversion factors

The intended audience for this System Requirements Specification (SyRS) includes:

- USDOT
- Transportation managers (including state and local Departments of Transportation (DOTs))
- Vehicle manufacturers and other device manufacturers or software developers
- Information service providers
- Fleet managers
- Commercial vehicle operators and regulators
- Application developers
- Potential Core System acquirers, deployers, operators, and maintainers.

1.3 System Overview

The USDOT's *connected vehicle* program envisions the combination of applications, services and systems necessary to provide safety, mobility and environmental benefits through the exchange of data between mobile and fixed transportation users. It consists of the following:

- **Applications** that provide functionality to realize safety, mobility and environmental benefits,
- **Communications** that facilitate data exchange, and
- **Core Systems**, which provide the functionality needed to enable data exchange between and among mobile and fixed transportation users.

The Core System's main mission is to enable safety, mobility and environmental communications-based applications for both mobile and non-mobile users. The scope of the Core System includes those enabling technologies and services that will in turn provide the foundation for applications. The system boundary for the Core System is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behavior of all interactions between Core System Users.

The Core System supports a distributed, diverse set of applications. These applications use both wireless and wireline communications to provide:

- Wireless communications with and between mobile elements including vehicles (of all types), pedestrians, cyclists, and other transportation users
- Wireless communications between mobile elements and field infrastructure
- Wireless and wireline communications between mobile elements, field infrastructure, and back office/centers

The Federal Communications Commission (FCC) allocated 75 Megahertz (MHz) of spectrum in the 5.9 Gigahertz (GHz) frequency range for the primary purpose of improving transportation safety. In addition to safety of life and public safety applications, the FCC's Final Report and Order also allowed private and non-safety applications to make use of the spectrum on a lower priority basis. This allowed the VII program and associated research efforts to test the capabilities of 5.9 GHz DSRC for vehicular based safety and mobility applications.

VII considered that some safety and mobility applications would be installed on all participating vehicles. Some safety applications would have been mandated to be installed on participating vehicles. Non-safety or mobility applications would have been installed on an opt-in basis however. The work following VII retains those possibilities that some applications may be mandated for safety while others would be optional.

A critical factor driving the conceptual view of the Core System and the entire *connected vehicle* environment is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, but not necessarily exclusively through anonymous communication. The Core System is planning anonymity into the trusted exchange of data, using the existing privacy principles[1] as guidelines, and balancing privacy against security and safety.

While the Core System is being planned for anonymity, it is also providing a foundation from which to leverage alternative communications methods for non-safety applications. These alternatives are typically available on the market today and the levels of anonymity and privacy inherent to these systems are typically governed by agreements between communication providers and consumers. So, while privacy is not compromised for an individual, what happens between that individual and their communication provider (e.g., 3G service provider) very well may compromise privacy. Some application providers may require personal information in order to function which would require the Application User to opt-in to use that application.

VII was conceived as a nationally deployed and managed system but the current thinking is that the *connected vehicle* system will likely be deployed locally and regionally and it must be able to grow organically to support the changing needs of its user base. Deployments will likely be

[1] VII Privacy Policies Framework version 1.0.2

managed regionally but will need to follow national standards to ensure that the essential capabilities are compatible no matter where the deployments are established.

Within the *connected vehicle* environment the Core System concept distinguishes communications mechanisms from data exchange and from the services needed to facilitate the data exchange. The Core System supports the *connected vehicle* environment by being responsible for providing the services needed to facilitate the data exchanges. The contents of the data exchange are determined by applications unless the data exchange is used as part of the facilitation process between the user and the Core System.

The Core System provides the functionality required to support safety, mobility, and environmental applications. This same functionality may enable commercial applications, but that is not a driving factor, rather a side effect. The primary function of the Core System is the facilitation of communications between users, some of which must also be secure. The Core System may also provide data distribution and network support services depending on the needs of the Core System deployment.

The Core System exists in an environment where it facilitates interactions between vehicles, field infrastructure and backoffice users, as illustrated in Figure 1-1 below.

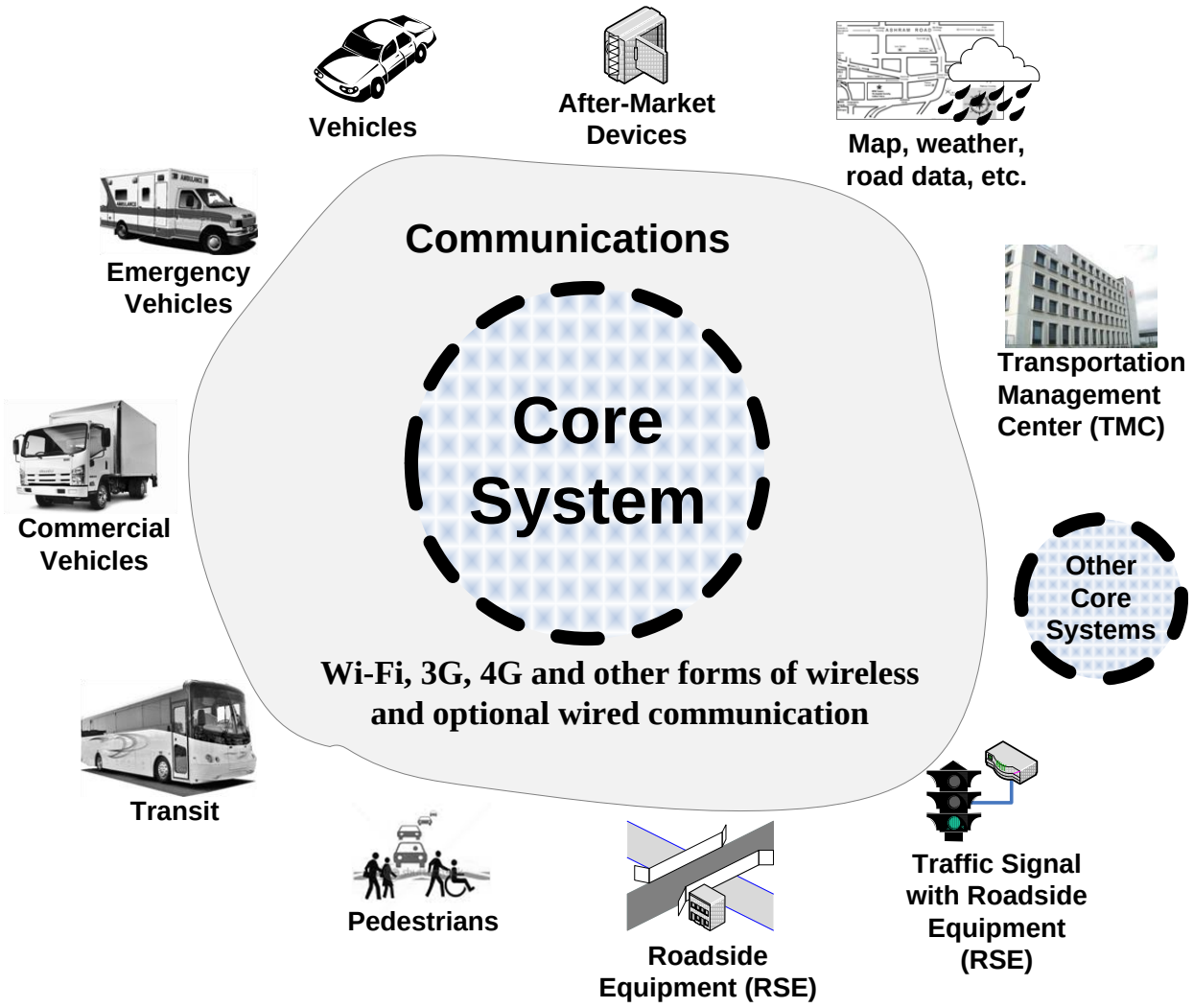


Figure 1-1. Core System Boundary Diagram

In Figure 1-1 above, the users, devices, and software applications are outside of the Core System but the Core System is still responsible for facilitating their security which is chiefly done by providing digital certificate-based mechanisms to ensure trust between users. The Core System also provides networking services to facilitate communications, though it does not comprise the communications network. Readers who are familiar with VII should note that the following are not part of the Core System:

- Mobile Users (e.g., vehicle devices, pedestrian smartphones) – any user device.
- Roadside Equipment (RSE) – both public and commercial fixed devices.
- Transportation Management Centers (TMC) and other public or private backoffice or centers

It is also important to note that the Core System is not meant to mandate or change existing transportation equipment, technology or transportation centers. The Core System provides mechanisms for efficiently collecting and distributing transportation data, but does not

necessarily replace existing systems, though it is likely that many existing data collection mechanisms will be made obsolete by its data collection and distribution function.

Figure 1-2 below shows the context in which the Core System operates as part of the overall connected vehicle environment. The center, field, and mobile systems interact with the Core System as do other Core Systems and external support systems. The center, field, and mobile systems also each other either independently of the Core or, in some cases, enabled by the security services provided by the Core.

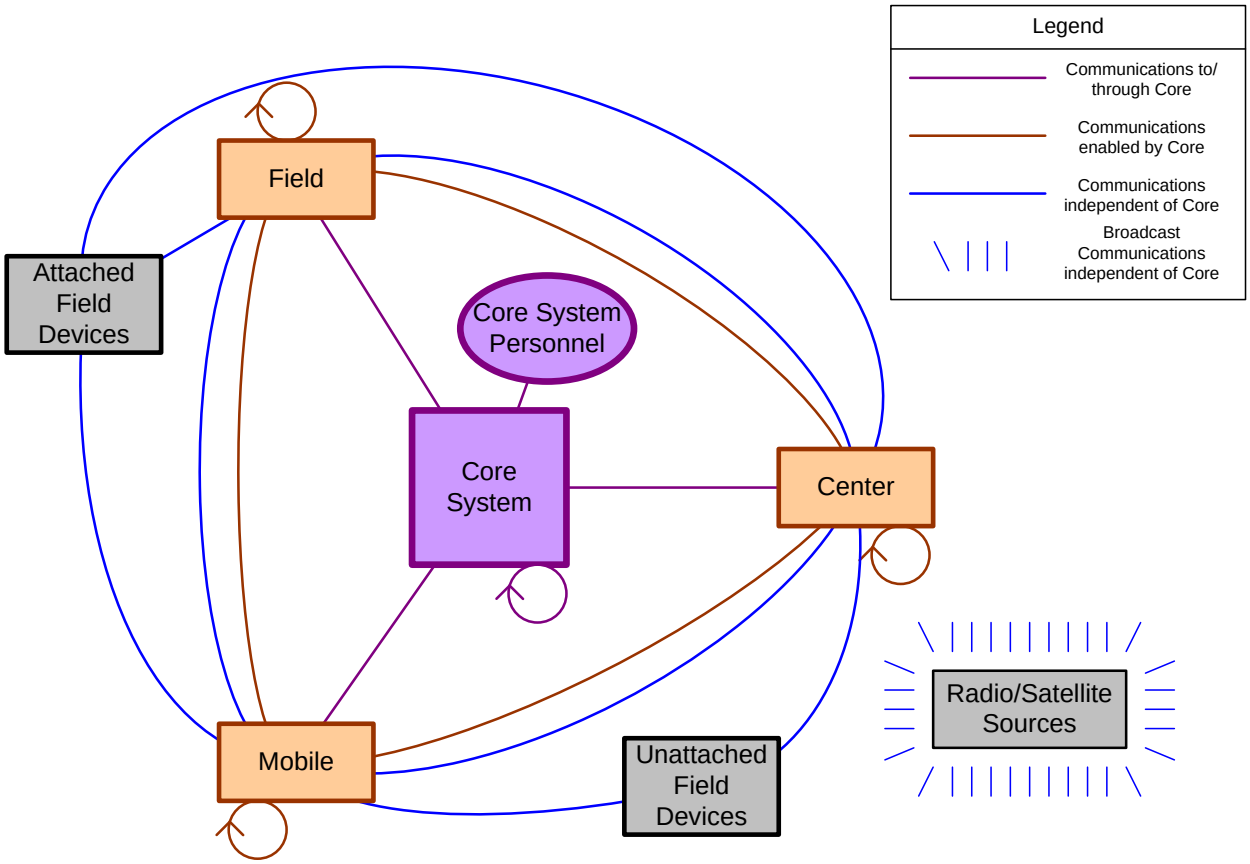


Figure 1-2. Core System Context Diagram

The diagram shown below in Figure 1-3 illustrates the context in which the Core System operates from the perspective of subsystems it contains and its interaction with the outside. The Core System includes eight subsystems and it interacts with Field, Mobile, and Center Users, other Core Systems, External Support Systems and Core System Operators.

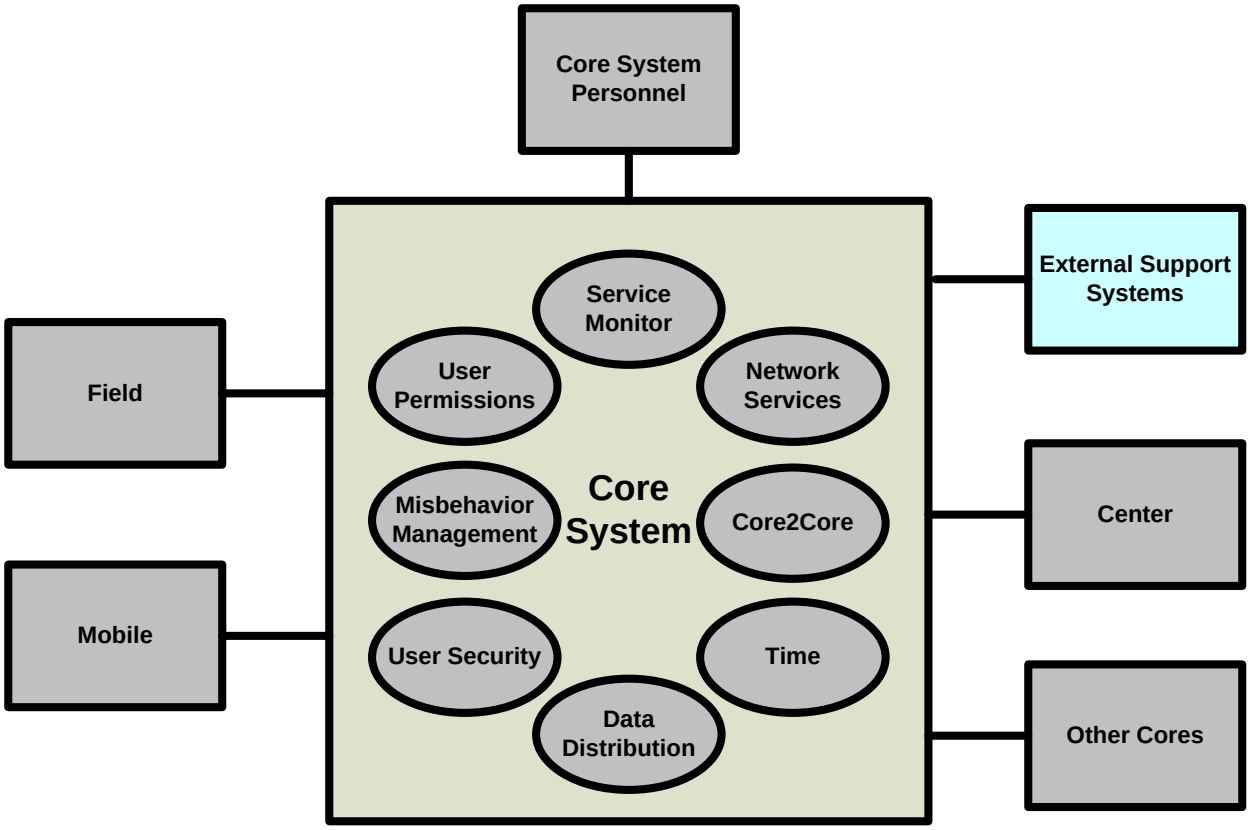


Figure 1-3. Core System Subsystem Context

The following provides a description of each of the subsystems of the Core System arranged alphabetically. A subsystem is defined as an integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses[2]. The requirements have been organized around this set of subsystems.

Core2Core Subsystem: The Core2Core Subsystem interfaces with other Core Systems, declaring its jurisdictional scope, offered services, and services it desires from other Cores. The Core2Core subsystem will maintain a knowledge base of data and services available among other Cores. In this way the Core System can act as a System User to another Core System, providing proxy services that it does not offer but another Core does. Additionally, Core2Core is responsible for compatibility between Cores, ensuring that one Core does not encroach on the scope of another Core, and similarly accepting error messages from Mobile Users that might indicate a cross-jurisdictional compatibility or scope coverage issue. Interfaces between Cores will be formalized in interfaces specifications. Conflicts and discrepancies between Cores will have to be resolved by agreements between the organizations responsible for the respective Cores.

[2] INCOSE Systems Engineering Handbook v3.1, The Hierarchy within a System, Appendix E-1.

Data Distribution Subsystem: The Data Distribution Subsystem maintains a directory of System Users that want data and facilitates the delivery of that data to those users. It supports multiple distribution mechanisms, including:

- Source-to-Points: The data provider communicates data directly to data consumers. In this case no data is sent to the Core System, however the Core is involved to check System User Permissions and to provide addressing services through those subsystems
- Publish-Subscribe: The data provider communicates data to the Data Distribution subsystem, which forwards it to all users that are subscribed to receive the data.

Data Distribution allows data consumers to specify (and change the specification of) data they wish to receive using criteria including:

- Data type
- Data quality characteristics
- Data format requirements
- Geographic area
- Sampling rate
- Minimum and maximum frequency of data forwarding

Data Distribution maintains a registry of which data consumers get what data according to the criteria defined above. Data Distribution Publish-Subscribe does not store or buffer data beyond that which is necessary to complete publish-subscribe actions. If a given data consumer is unable to receive data that it has subscribed to because of a communications or other system failure, the data in question may be lost. The degree to which data distribution buffering accommodates connectivity failures will be up to the Core System deployment. Some Cores may offer "temporary storage" in this fashion.

Data Distribution repackages data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Data Distribution will also maintain source-to-points information. With this option, the data consumer will connect directly to the data provider with the address supplied by the Data Distribution subsystem. When connected, the data provider sends the data directly to each consumer bypassing the Core System.

Data Distribution does not share or exchange data with other Core Systems. System Users that want data from multiple Cores need to subscribe to each Core.

Misbehavior Management Subsystem: The Misbehavior Management Subsystem analyzes messages sent to the Core System to identify users operating outside of their assigned permissions. It works with the User Permissions subsystem to identify suspicious requests and to maintain a record of specifically identifiable users that:

1. Provide false or misleading data
2. Operate in such a fashion as to impede other users
3. Operate outside of their authorized scope

Because most end users will rarely interface with the Core System, Misbehavior Management will also accept reports of misbehaving users from other users. Center, Mobile, and Field users can send misbehavior reports that reference credentials attached to messages and note the type of

misbehavior in question. Misbehavior Management will record such reports and according to a set of Core System Personnel-controlled rules will determine when to revoke credentials from such reported misbehaving users. For anonymous users revocation is more complex and may result instead in a lack of credential renewal. Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

Network Services Subsystem: The Network Services Subsystem provides information to System Users and Core System services that enable communication between those users and services. The Network Services subsystem will provide the information necessary for users to communicate with other users that have given permission to be communicated with. Network Services will also provide the information necessary to enable users to communicate with a group of users by maintaining information regarding available communications methods, addresses, and performance characteristics for geo-cast communications.

Network Services will also provide management for Communications Layer resources. It will enable decisions about which communications medium to use when more than one is available. This includes identifying available communications methods current performance characteristics and applicable user permission levels. Permission requirements will be coordinated with the User Permissions subsystem.

Service Monitor Subsystem: The Service Monitor Subsystem monitors the status of Core System services, interfaces, and communications networks connected to the Core. It informs System Users of the availability and status of its services.

Service Monitor also monitors the integrity of internal Core System components and supporting software, and mitigates against vulnerabilities. This includes periodic verification of the authenticity of Core service software and supporting software. This also includes monitoring for vulnerabilities including but not limited to virus protection, network port monitoring, and monitoring for patches to third party components. Should a vulnerability be detected or a component of the Core found to have lost integrity, Service Monitor takes steps to mitigate against damage and performance degradation.

The Service Monitor Subsystem ensures the physical security of Core System services by monitoring the environmental conditions that Core components operate in (e.g. temperature and humidity) as well as the condition of its power system. It takes steps to mitigate against system failures in the event that environmental conditions exceed operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of Core service operations, as well as Core System Personnel (Core System staff) notification.

Service Monitor also monitors the performance of all services and interfaces and makes performance metrics available to Core System Personnel (Core System staff).

Time Subsystem: The Time Subsystem uses a time base available to all System Users and makes this time available to all Core System services which use this time base whenever a time reference is required.

User Permissions Subsystem: The User Permissions Subsystem provides tools allowing System Users to verify whether a given user, identified by digital certificate-based credentials, is authorized to request or perform the action requested in the message payload. It also maintains the status of users, whether they have a specific account, their allowed behaviors with defined

permissions (publish, subscribe, actions allowed to request, and administration etc.), or if they belong to an anonymous group. User Permissions provides the tools for Core System Personnel to: create new users and groups, modify existing users and groups, and modify permissions associated with users and groups.

User Security Subsystem: The User Security Subsystem manages access rules and credentials in the form of digital certificates (including X.509, 1609.2 identity. and 1609.2 anonymous certificates) for all System Users and Core System components that require and are entitled to them. It creates and distributes cryptographic keys to qualifying System Users. It works with User Permissions to determine whether a given user applying for credentials or keys is entitled to them. It also manages the revocation of credentials and the distribution of Certificate Revocation Lists (CRLs) of disallowed credentials to interested System Users. User Security may use an External Support System to manage certificates, but such a determination is a design decision and will be deferred until the system architecture is defined.

1.4 Stakeholders

The term “stakeholder” may be somewhat overused but generally refers to any individual or organization that is affected by the activities of a business process or, in this case, a system being developed. They may have a direct or indirect interest in the activity and their level of participation may vary. The term here includes public agencies, private organizations or the traveling public (end users) with a vested interest, or a "stake" in one or more aspect of the *connected vehicle* environment and this Core System. Core System stakeholders span the breadth of the transportation environment including:

- Transportation Users, e.g., private vehicle drivers, public safety vehicle operators, commercial vehicle operators, passengers, cyclists and pedestrians
- Transportation Operators, e.g. traffic managers, transit managers, fleet managers, toll operators, road maintenance and construction
- Public Safety organizations, e.g. incident and emergency management, including fire, police and medical support
- Information Service Providers, e.g. data and information providers for transportation-related data, including traffic, weather and convenience applications
- Environmental Managers, including emissions and air quality monitors
- Original Equipment vehicle Manufacturers (OEMs)
- In-vehicle device manufacturers
- Communications Providers, including cellular network operators
- Federal regulatory and research agencies under the umbrella of USDOT
- Core System owners.

2 Documents

This section identifies all needed standards, policies, laws, concept of operations, concept exploration documents and other reference material that supports the requirements.

This section is divided into two portions. The first section lists the documents that are explicitly referenced as part of this document. The second section lists the documents or other resources that were used for background information and as a source for potential requirements during the development of this SyRS though there may not be a direct reference.

2.1 Referenced Documents

- Core System Concept of Operations (ConOps), Rev C, April 19, 2011 and Walkthrough Comment Resolution Report.
- IEEE Std. 1233 – IEEE Guide for Developing System Requirements Specifications, 22 Dec 1998
- IEEE 1609.2 Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, June 2006. Note: This standard defines three types of end entities, or potential certificate holders: Identified, Identified Not Localized, and WAVE Service Announcement (WSA) Signer. It says that future versions of this standard will also define end entities of type Anonymous.
- IEEE 1609.4 Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operations, Oct 2006
- INCOSE Systems Engineering Handbook version 3.1, August 2007.
- Vehicle Infrastructure Integration (VII) USDOT Day-1 Use Case Descriptions, v1.0, May 2006
- Vehicle Infrastructure Integration Consortium (VIIC) Standards Recommendations, VIIC Document SYS090-05, May 23, 2010
- VII Concept of Operations (ConOps), BAH, v1.2, September-06
- VII National System Requirements (NSR), BAH, v1.3.1, April-08
- VII Privacy Policies Framework, Version 1.0.2, February 16, 2007

2.2 Resource Documents

- A Provisional Technical Architecture for the VII, PB Farradyne, July 2004
- A Summary of European Cooperative Vehicle Systems Research Projects, Jun-09
- Achieving the Vision: Policy White Paper, 4/30/2010
- An Initial Assessment of the Ability of 4G Cellular Technology to Support Active Safety Applications, Final Draft, 11/18/2009
- Architecture Specification for the Vehicle and Certificate Authority Certificate Management Subsystems, VIIC
- CAMP Security Final Report, Draft, 8/31/2010
- CEN TC278-WG16_ISO TC204-WG18_2nd Meeting-Sept-2010_ Agenda, 7/24/2010
- Certificate Authority (CA) Subsystem Specification, BAH, v1.1, February-07
- Certificate Management Concept of Operation, VIIC, SEC 110-01

- Cooperative Intersection Collision Avoidance System for Violations (CICAS-V) for Avoidance of Violation-Based Intersection Crashes Paper, Michael Maile and Luca Delgrossi, March 2009
- Data Element Dictionary, BAH, v1.0, February-07
- EC Standardization Mandate M/453 Preliminary work plan for ETSI TC ITS, 7/27/2010
- Enterprise Network Operations Center (ENOC) Subsystem Specification, BAH, v1.1
- ETSI Intelligent Transport Systems (ITS) Security Services and Architecture, ETSI TS 102 731, v1.1.1, 9/21/2010
- European ITS Framework Architecture, v4.0, 2009
- European ITS Communication Architecture, v3.0, 2010
- Final Report: VII POC Executive Summary – Infrastructure (Volume 1B), BAH
- Final Report: VII POC Executive Summary – Vehicles (Volume 1A), VIIC
- Final Report: VII POC Results and Findings – Infrastructure (Volume 3B), BAH
- Final Report: VII POC Results and Findings – Vehicles (Volume 3A), VIIC
- Final Report: VII POC Technical Description – Infrastructure (Volume 2B), BAH, 5-15-09 Final
- Final Report: VII POC Technical Description – Vehicles (Volume 2A), VIIC, volume 2
- Functional and Performance Requirements for the VII POC OBE Subsystem, VIIC
- IEEE P1609 Working Group Meeting Notice and Draft Agenda, 7/14/2010
- IEEE 1609.1 Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager, Oct 2006
- IEEE 1609.3 Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, Apr 2007
- IEEE 802.11p-2010, 15 July 2010
- IEEE Standard 802.16: A Technical Overview, C80216-02_05, 6/4/2002
- IEEE Standard for Software Configuration Management Plans, 12 Aug 2010
- IEEE Std. 1028-1997 – IEEE Standard for Software Reviews, 9 December 1997
- IEEE Std. 1220-2005 – IEEE Standard for Application and Management of Systems Engineering Process, 9 September 2005
- Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994
- Infrastructure Lexicon, BAH, v1.1, February-07
- Intelligent Transport Systems (ITS) Communications Architecture, ETSI EN 302 665 V1.1.1 (2010-09), European Telecommunications Standards Institute 2010.
- Internet Official Protocol Standards, RFC 5000, Internet Engineering Task Force (IETF) May 2008
- Internet Protocol Defense Advanced Research Projects Agency (DARPA) Internet Program Protocol Specification, RFC 791, Internet Engineering Task Force (IETF), Sept 1981.
- ITS Standards Development Organizations Membership Overlap Analysis, Jan-10
- ITS Strategic Research Plan, 2010-2014: Executive Summary, US DOT, 3/29/2010
- Joint CEN and ETSI Response to Mandate M/453 – EC Comments, 7/27/2010
- M/453 Co-operative Systems Progress Report, 7/27/2010
- Mileage-based User Fee Technology Study, 8/7/2009

- Network Subsystem Specification Addendum, BAH, v1.0.1a, March-07
- Network Subsystem Specification, BAH, v1.1, April-07
- OBE Communications Manager Subsystem Requirements Specification, VIIC, ENA 110-02
- OBE Subsystem Design Description, VIIC, SYS 112-02 (OBE), SYS 112-01
- OBE to RSE Interface Requirements Specification, VIIC, SYS 120-04
- POC OBE Subsystem Functional and Performance Requirements, VIIC, SYS 110-02
- POC Probe Data Collection Vehicle Application Requirements, VIIC, APP 220-01
- POC Trippath Generation Application Requirements, VIIC, APP 220-04
- Policy Roadmap for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Safety, Draft: 05/19/2010
- Potential Haul-In Aftermarket Device Suppliers, 6/11/2010
- Requirements for Internet Hosts – Application and Support, RFC 1123, Internet Engineering Task Force (IETF), Oct 1989
- Requirements for Internet Hosts – Communications Layers, RFC 1122, Internet Engineering Task Force (IETF), Oct 1989
- Risk Management Plan for the Deployment of IVI Collision Avoidance Safety Systems, Draft, Ver 1, 11/4/2004
- RSE Procurement Analysis, BAH, v1.0, June-06,
- Roadway Geometry and Inventory Trade Study for Applications, 7/1/2010
- RSE Software Requirements Specification (SRS), BAH, v2.0, July-07
- RSE Subsystem Specification, BAH, v1.2
- SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary, v2, Nov 2009
- SAE J2735 Standard: Applying the Systems Engineering Process, 6/30/2010
- Service Delivery Node (SDN) Subsystem Specification, version 1.1, February 2007
- Standardization Mandate
- Transit Crosscutting Application Development and Implementation Program Plan and Roadmap (2010-2014), 3.1, Jul-10
- US Code Section 36 CFR Part 1194 - Electronic and Information Technology Accessibility Standards (36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended), Dec. 21, 2000
- USDOT Federal Highway Administration (FHWA) and California Department of Transportation (CalTRANS) Systems Engineering Guidebook, version 3, Dec 2, 2009.
- Vehicle Safety Communications – Applications (VSC-A) Project: Crash Scenarios and Safety Applications, Michael Maile, May 2, 2007
- Vehicle Safety Communications in the United States Paper, Michael Shulman and Richard Deering, March 2007
- Vehicle Segment Certificate Management Concept of Operations, VIIC, SEC 110_01
- Vehicle Segment Security Plan (Security ConOps), SEC 100-10, Jan 2007
- Vehicle-Vehicle and Vehicle-Infrastructure Communications based Safety Applications, Michael Maile, February 2010
- VII Architecture and Functional Requirements, PB Farradyne, VII Architecture version 1.1 2005_07_20

- VII Communications Analysis Report, BAH, v3.0, July-06
- VII System Discussion, 7/8/2010
- VII USDOT Day-1 Use Case Descriptions, BAH, Combined Final v1.0, May-06
- X-072 Interface Requirements Specification, SYS 120-02

3 Requirements

This section of the document lists the Core System Requirements. The requirements are organized first by level, i.e. system vs. subsystem. The System level requirements then are divided into the following types:

1) Functional — The Functional requirements specify actionable behaviors of the Core System.
2) Performance — The Performance requirements specify quantifiable characteristics of Core System operations.
3) Interface — The Interface requirements define the Core System external interfaces to non-Core Systems (the outside world).
4) Data — The Data requirements define the data stored within the Core System.
5) Non-Functional — The Non-Functional requirements define the characteristics of the overall operation of the system such as reliability, maintainability, safety, and environmental [e.g. temperature] requirements.
6) Enabling — The Enabling requirements describe the production, development, testing, training, support, deployment, and disposal.
7) Constraints — The Constraints requirements pertain to how the Core System will be built and deployed.

The subsystem requirements that follow are based on the subsystems identified in the Core System ConOps and are then divided into the following types:

1) Functional — The Functional requirements specify actionable behaviors of the subsystems.
2) Performance — The Performance requirements specify quantifiable characteristics of the operations of that subsystem.
3) Interface — The Interface requirements define the external interfaces to non-Core Systems (the outside world) as well as to other subsystems within the Core System. Section 5.5 on page 74 for a table showing the internal interfaces.
4) Data — The Data requirements define the data stored within the subsystem.

Section 5.4 on page 70 defines the action verbs that are used in the requirements.

3.1 System Requirements

This section provides the high-level requirements for the Core System, i.e. “What the system shall do”. They are organized by the types of requirements and are related to the Needs identified in the ConOps.

3.1.1 System Functional Requirements

This section provides the functional requirements for the Core System, i.e. “What the system shall do”.

3.1.1.1 The Core System shall be configured to a geographic boundary of its services for System Users.
3.1.1.2 The Core System subsystems shall send status to the Service Monitor Subsystem.
3.1.1.4 The Core System subsystems shall transition to degraded mode upon a failure.
3.1.1.5 The Core System subsystems shall accept requests from an authorized System Operator to transition the Core System subsystem's mode.
3.1.1.6 The Core System subsystems shall accept requests from an authorized System Operator to transition the Core System subsystem's state.
3.1.1.7 The Core System shall validate its configuration with interfacing Core Systems.
3.1.1.8 The Core System shall accept error messages from System Users.
3.1.1.9 The Core System shall validate trust credentials with System Users.
3.1.1.10 The Core System shall provide a history of System User's accesses to the Core System.
3.1.1.11 The Core System shall provide a list of available services to System Users.
3.1.1.12 The Core System shall identify misbehavior with System Users.
3.1.1.13 The Core System shall provide a backup capability with interfacing Core Systems.
3.1.1.14 The Core System shall provide data forwarding capability to System Users.
3.1.1.15 The Core System shall provide a secure storage capability to protect data.
3.1.1.16 The Core System shall accept System User's requests to receive data.
3.1.1.17 The Core System shall maintain a catalog of data providers.
3.1.1.18 The Core System shall accept requests to publish data from System Users.
3.1.1.19 The Core System shall validate user permissions with System Users.
3.1.1.20 The Core System shall manage information on data publishers.
3.1.1.21 The Core System shall provide an interface to an authorized System Operator to configure the Publisher/Subscriber data configuration.
3.1.1.22 The Core System shall provide an interface to an authorized System Operator to configure the source-to-point data configuration.
3.1.1.23 The Core System subsystems shall send state information to the Service Monitor Subsystem.
3.1.1.24 The Core System subsystems shall accept time of day from the Time Subsystem
3.1.1.25 The Core System shall receive misbehavior reports from System Users.
3.1.1.26 The Core System shall accept requests from an authorized System Operator to configure correlation processing.
3.1.1.27 The Core System shall send reports to an authorized System Operator identifying misbehavior of the Core System.
3.1.1.28 The Core System shall provide message distribution based on geographical location.
3.1.1.29 The Core System shall manage status of the Core System.
3.1.1.30 The Core System shall provide a list of available Core System services to other Core Systems.
3.1.1.31 The Core System shall manage the health of the Core System.
3.1.1.32 The Core System shall manage the Core System software configuration.
3.1.1.33 The Core System shall manage Core System hardware configuration.
3.1.1.34 The Core System shall manage transitions between states of the Core System.
3.1.1.35 The Core System shall receive time from an external source.
3.1.1.36 The Core System shall synchronize time to the Core System subsystems.
3.1.1.37 The Core System shall validate user permissions with System Users.
3.1.1.38 The Core System shall validate user permissions with Core System Personnel.
3.1.1.39 The Core System shall validate the System User's certificate(s).
3.1.1.40 The Core System shall validate messages from System Users.

3.1.1.41 The Core System shall manage IEEE 1609.2 Certificate Authority functions for System Users.
3.1.1.42 The Core System shall manage X.509 Certificate Authority functions for System Users.
3.1.1.43 The Core System shall provide an interface to an authorized System Operator to manage X.509 Certificate Authority functions.
3.1.1.44 The Core System shall provide an interface to an authorized System Operator to manage IEEE 1609.2 Certificate Authority functions.
3.1.1.45 The Core System shall provide an interface to an authorized System Operator to manage Certificate Authority (CA) locations.
3.1.1.46 The Core System shall manage 1609.2 Certificates to System Users.

3.1.2 System Performance Requirements

3.1.2.1 The Core System shall synchronize status from other Core Systems it interfaces with every 5 minutes (TBD) to check availability.
3.1.2.2 The Core System subsystems shall send a message within 30 seconds[TBD] to all interfacing Core Systems upon any state change.
3.1.2.3 The Core System shall buffer forwarding data with a latency no greater than 500ms[TBD].
3.1.2.4 The Core System shall process up to [TBD] misbehavior reports per minute from System Users.
3.1.2.5 The Core System shall perform the misbehavior report correlation processing [TBD] times per hour.
3.1.2.6 The Core System geocast service shall support up to [TBD] geocast sessions at any given time.
3.1.2.7 The Core System geocast service shall support up to [TBD] megabits per second (Mbps) per geocast stream.
3.1.2.8 The Core System shall notify an authorized System Operator within 30 seconds upon a failure.
3.1.2.9 The time of day shall not drift (lagging or leading in time) from the external time source standard time reference by more than [TBD] 1 second per year.
3.1.2.10 The Core System shall synchronize the time of day with all the Core Subsystems every 10ms (TBD).
3.1.2.11 Upon request, the Core System shall provide Core System Personnel registration information to other Core System subsystems with [TBD] seconds.
3.1.2.12 Upon request, the Core System shall provide Core System Personnel user permissions information to other Core System subsystems with [TBD] seconds.
3.1.2.13 Upon request from an authorized System Operator, the Core System shall provide System User registration information to other Core System subsystems within [TBD] seconds.
3.1.2.14 Upon request from an authorized System Operator, the Core System shall provide System User permissions information to other Core System subsystems within [TBD] seconds.
3.1.2.15 The Core System shall process up to [TBD] 1609.2 Certificate Requests per second from System Users.
3.1.2.16 The Core System shall process up to [TBD] X.509 Certificate Requests per minute from System Users.
3.1.2.17 The Core System shall generate 1609.2 Certificate Revocation Lists (CRL) periodically at [TBD] rate.
3.1.2.18 The Core System shall generate X.509 Certificate Revocation Lists (CRL) periodically at [TBD] rate.
3.1.2.19 The Core System's subsystems shall periodically send their operational state to the Service Monitor Subsystem every 500ms. Note: this also represents a heartbeat.

3.1.3 System Interface Requirements

3.1.3.1 The Core System shall interface with other Core Systems.
3.1.3.2 The Core System shall interface to System Users for data distribution.
3.1.3.3 The Core System shall interface to System Users for misbehavior management.
3.1.3.4 The Core System shall interface to System Users to provide status information.
3.1.3.5 The Core System shall interface to a real-time external time source to provide time synchronization with the Core System.

3.1.3.6 The Core System shall interface to an authorized System Operator Administrator to support user permission configuration.
3.1.3.7 The Core System shall interface to System Users.
3.1.3.8 The Core System shall interface to System Users for 1609.2 Certificates.
3.1.3.9 The Core System shall interface to System Users for X.509 Certificates.
3.1.3.10 The Core System shall provide internal interfaces to decoupled Core System services for a distributed system.
3.1.3.11 The Core System shall support an Internet interface to connect to System Users.

3.1.4 System Data Requirements

3.1.4.1 The Core System shall maintain a knowledge base of interfacing Core Systems.
3.1.4.2 The Core System shall maintain a registry of publisher information.
3.1.4.3 The Core System shall maintain a registry of data requester information.
3.1.4.4 The Core System shall maintain a registry of misbehavior information.
3.1.4.5 The Core System shall store Core System subsystems status.
3.1.4.6 The Core System shall store Core System subsystems states.
3.1.4.7 The Core System shall store interfacing Core System(s) status.
3.1.4.8 The Core System shall store System User's permission information.
3.1.4.9 The Core System shall store System User's Certificate information.
3.1.4.10 The Core System shall store Certificate Revocation Lists (CRL).

3.1.5 Non-functional Requirements

3.1.5.1 Physical Security

3.1.5.1.1 The Core System shall be enclosed in a secure facility for authorized personnel only.
3.1.5.1.2 The Core System shall validate user’s authorization upon entering the facility.
3.1.5.1.3 The Core System's facility shall be protected by physical access controls.
3.1.5.1.4 The Core System's facility shall log physical access attempts.

3.1.5.2 Environmental Features

3.1.5.2.1 The Core System shall operate in an environmentally safe facility.
3.1.5.2.2 The Core System's facility shall operate when exposed to a relative humidity up to 95%, including condensation.
3.1.5.2.3 The Core System's facility shall operate in ambient temperatures from 0*C (32*F) to 40*C (104*F).
3.1.5.2.4 The facility housing the Core System's equipment shall have an air-conditioning system capable of providing a relative humidity of 45-50%.
3.1.5.2.5 The facility housing the Core System's equipment shall not vary the relative humidity more than 10% per hour of operation.
3.1.5.2.6 The facility housing the Core System's equipment shall have heat and smoke detectors that meet or exceed all local fire code regulations.

3.1.5.3 Backup Power

3.1.5.3.1 The Core System shall operate in case of power failure.
3.1.5.3.2 The Core System shall provide sufficient backup power capacity capable of supporting the Core System up to 4 hours [TBD].

3.1.5.3.3 The facility housing the Core System's equipment shall allow for the network equipment racks to be electrically grounded.

3.1.5.4 Availability

3.1.5.4.1 The Core System shall be available in normal operational state 99.5% of the time (an average of less than one hour per week or 1.83 days per year).

3.1.5.5 Maintainability

3.1.5.5.1 The Core System's Mean Time To Repair (MTTR) shall not exceed 3.0 hours [TBD].

3.1.5.5.2 The Core System Mean Time Between Failures (MTBF) shall be greater than 1500 hours (62.5 days) [TBD].

3.1.6 Enabling Requirements

These include production, development, testing, training, support, deployment, and disposal of the fielded system. At this time in the evolution of the Core System there are no enabling requirements. They will be developed as choices are made in how the system will be implemented and fielded.

3.1.6.1 The Core System shall transition to Training State when commanded by an authorized System Operator.

3.1.6.2 During Training State, each Core System subsystems shall be allowed to display real-time log messages.

3.1.6.3 During Training State, each Core System subsystems shall be allowed to provide debug messages.

3.1.6.4 During Training State, the Core2Core Subsystem shall be disabled.

3.1.7 Constraints

This section describes requirements pertaining to how the Core System will be built and deployed (e.g. Technology, design, tools, and/or standards). A constraint is a factor that lies outside, but has a direct impact on, a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.

3.1.7.1 The Core System shall conform to the privacy principles as defined in the VII Privacy Policies Framework regarding the use of personal information.

3.1.7.2 The IEEE 1609.x family of standards (including 1609.1, 1609.2, 1609.3 and 1609.4) shall serve as the interface standards for 5.9GHz DSRC.

3.1.7.3 The X.509 certificates shall provide the basis for Core and System User non-DSRC certificates.

3.1.7.4 The SAE 2735 standard shall serve as the basis for messages exchanges from Mobile Users.

3.1.7.5 The public sector transportation agencies shall use existing personnel to operate the Core System. Note: It was a consistent theme from public sector personnel that most existing public sector transportation agencies cannot afford additional personnel for the Core System.

3.1.7.6 When a Core System service requires geo-referencing, the same geo-referencing capabilities shall be available to all System Users. Note: otherwise it will be difficult or impossible to coordinate location references, jeopardizing safety and mobility applications that depend on accurate positioning data.

3.1.7.7 Service performance characteristics of the Core System shall be constrained by the communications technology with which users connect to Core System. Note: minimum performance standards can be

set for usage by the Core System services, but is constrained by what is technically available at the time. Unless DSRC field infrastructure is deployed at a pace sufficient to keep up with Core System and Mobile User deployments, usage of existing communications infrastructure, particularly 3G and 4G cellular, may be required to deliver services.

3.1.7.8 External interfaces on Core System shall be defined as open standards.

3.1.7.9 IPv6 shall provide the basis for communications between System Users not communicating with DSRC. Note: IPv4 is being phased out and will not be supported.

3.2 Subsystem Requirements

This section provides the requirements for each of the subsystems within the Core System as described in the ConOps and are divided by the type of requirements: functional, performance, interface, and data.

3.2.1 Core2Core Subsystem

The Core2Core Subsystem interfaces with other Core Systems, declaring its jurisdictional scope, offered services, and services it desires from other Cores. The Core2Core subsystem will maintain a knowledge base of data and services available among other Cores. In this way the Core System can act as a System User to another Core System, providing proxy services that it does not offer but another Core does. Additionally, Core2Core is responsible for compatibility between Cores, ensuring that one Core does not encroach on the scope of another Core, and similarly accepting error messages from Mobile Users that might indicate a cross-jurisdictional compatibility or scope coverage issue. Interfaces between Cores will be formalized in interfaces specifications. Conflicts and discrepancies between Cores will have to be resolved by agreements between the organizations responsible for the respective Cores.

3.2.1.1 Functional Requirements

3.2.1.1.1 The Core2Core Subsystem shall identify the geographic information describing the boundaries that it will service.

3.2.1.1.2 The Core2Core Subsystem shall identify the services that it will offer.

3.2.1.1.3 The Core2Core Subsystem shall provide information describing the communications that the Core System provides.

3.2.1.1.4 The Core2Core Subsystem shall accept a request from System Users for the geographic coverage area over which the Core System is servicing.

3.2.1.1.5 The Core2Core Subsystem shall send a response to a System User's request for the geographic coverage area over which the Core System is servicing.

3.2.1.1.6 The Core2Core Subsystems shall send status to the Service Monitor Subsystem.

3.2.1.1.7 The Core2Core Subsystem shall accept the time of day from the Time Subsystem.

3.2.1.1.8 The Core2Core Subsystem shall transition to degraded mode of operations when a hardware failure within the Core2Core Subsystem is detected.

3.2.1.1.9 The Core2Core Subsystem shall transition to degraded mode of operations when a software failure within the Core2Core Subsystem is detected.

3.2.1.1.10 The Core2Core Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.1.1.11 The Core2Core Subsystem shall transition to the requested state when commanded by an authorized System Operator.

3.2.1.1.12 The Core2Core Subsystem shall compare Software versions from its local Service Monitor to its interfacing Core Systems for compatibility.

3.2.1.1.13	The Core2Core Subsystem shall compare Hardware versions from its local Service Monitor to its interfacing Core Systems for compatibility.
3.2.1.1.14	The Core2Core Subsystem shall notify the Service Monitor when other Core Systems are not compatible.
3.2.1.1.15	The Core System shall accept an error message from a Mobile User when the Core System falsely advertises that a service as available, but is actually unavailable to the Mobile User.
3.2.1.1.16	The Core2Core Subsystem shall verify all trust credentials before exchanging information with interfacing Core Systems.
3.2.1.1.17	The Core2Core Subsystem shall send trust credentials to interfacing Core Systems before exchanging information.
3.2.1.1.18	The Core2Core Subsystem shall maintain a history of accesses to interfacing Core Systems.
3.2.1.1.19	The Core2Core Subsystem shall maintain a history of failed access attempts to other Core Systems.
3.2.1.1.20	The Core2Core Subsystem shall send interfacing Core Systems the software versions of the Core System currently running in operation.
3.2.1.1.21	The Core2Core Subsystem shall send the implemented versions of standards to the interfacing Core Systems.
3.2.1.1.22	The Core2Core Subsystem shall provide the list of available services to interfacing Core Systems, so that the interfacing Core System can advertise what services the other Core System has to offer.
3.2.1.1.23	The Core2Core Subsystem shall send the status of services offered to interfacing Core Systems to System Users.
3.2.1.1.24	The Core2Core Subsystem shall receive misbehavior information from other Core Systems.
3.2.1.1.25	The Core2Core Subsystem shall store information regarding misbehavior reports from other Core Systems.
3.2.1.1.25.1	The Core2Core Subsystem shall send misbehavior information to interfacing Core System.
3.2.1.1.26	The Core2Core Subsystem shall maintain information about interfacing Core Systems.
3.2.1.1.26.1	The Core2Core Subsystem shall maintain information regarding services offered by interfacing Core Systems.
3.2.1.1.26.2	The Core2Core Subsystem shall maintain information regarding the status of services offered by interfacing Core Systems.
3.2.1.1.26.3	The Core2Core Subsystem shall maintain information regarding the performance of services offered by interfacing Core Systems.
3.2.1.1.26.4	The Core2Core Subsystem shall protect its integrity from integrity issues with interfacing Core Systems.
3.2.1.1.27	The Core2Core Subsystem shall provide backup services to an interfacing degraded Core System.
3.2.1.1.27.1	The Core2Core Subsystem shall accept data stores from preselected interfacing Core Systems.
3.2.1.1.27.2	The Core2Core Subsystem shall send data stores for facility backup to preselected interfacing Core Systems.
3.2.1.1.27.3	The Core2Core Subsystem shall accept requests to operate as facility backup to preselected interfacing Core Systems.
3.2.1.1.27.4	The Core2Core Subsystem shall send requests to operate as facility backup to preselected interfacing Core Systems.
3.2.1.1.27.5	The Core2Core Subsystem shall provide facility backup of a variable subset of Core System services in the case of partially unavailability to an interfacing Core System.
3.2.1.1.27.6	The Core2Core Subsystem shall provide backup services to an interfacing failed Core System.
3.2.1.1.27.7	The Core2Core Subsystem shall accept requests to send certificates with interfacing Core Systems.
3.2.1.1.27.8	The Core2Core Subsystem shall send certificates upon request, with interfacing Core Systems.
3.2.1.1.28	The Core2Core Subsystem shall provide data forwarding services to preselected interfacing Core Systems at the System Operator's option.
3.2.1.1.28.1	The Core2Core Subsystem shall store information required to identify the proper interfacing Core System to which data can be forwarded.
3.2.1.1.28.2	The Core2Core Subsystem shall forward preselected data types to interfacing Core Systems for data provision.
3.2.1.1.28.3	The Core2Core Subsystem shall forward preselected data types to interfacing Core Systems for data request.
3.2.1.1.28.4	The Core2Core Subsystem shall forward preselected data types to interfacing Core Systems for data forward.

3.2.1.1.29 The Core2Core Subsystem shall coordinate coverage with interfacing Core Systems.
3.2.1.1.29.1 The Core2Core Subsystem shall advertise the boundaries of its service provision with interfacing Core Systems.
3.2.1.1.29.2 The Core2Core Subsystem shall coordinate the geographic boundaries that it will service with interfacing Core Systems.
3.2.1.1.30 The Core2Core Subsystem shall send its status to the Service Monitor Subsystem.
3.2.1.1.31 The Core2Core Subsystem shall receive reports from System Users indicating issues with another Core System.
3.2.1.1.32 The Core2Core Subsystem shall receive reports from System Users indicating compatibility issues with another Core System.
3.2.1.1.33 The Core2Core Subsystem shall receive reports from System Users indicating scope issues with another Core System.

3.2.1.2 Performance Requirements

3.2.1.2.1 The Core2Core Subsystem shall synchronize status from Core Systems it interfaces with every 5 minutes (TBD) to check availability.
3.2.1.2.2 The Core2Core Subsystem shall send a message within 30 seconds[TBD] to all interfacing Core Systems upon any state change.

3.2.1.3 Interface Requirements

3.2.1.3.1 Core2Core External Interfaces
3.2.1.3.1.1 The Core2Core Subsystem shall establish persistent communications with interfacing Core Systems.
3.2.1.3.1.2 The Core2Core Subsystem shall support an interface to the System Operator to configure parameters that control the sharing of misbehavior information with interfacing Core Systems.
3.2.1.3.1.3 The Core2Core Subsystem shall support an interface to the System Operator to control what information to provide to each interfacing Core System.
3.2.1.3.1.4 The Core2Core Subsystem shall support an interface to System Operators to select services to be offered to interfacing Core Systems.
3.2.1.3.2 Core2Core Internal Interfaces
3.2.1.3.2.1 The Core2Core Subsystem shall interface with the Data Distribution Subsystem for sharing data provisioning information to a backup Core System.
3.2.1.3.2.2 The Core2Core Subsystem shall interface with the Misbehavior Management Subsystem for misbehavior management.
3.2.1.3.2.3 The Core2Core Subsystem shall interface with the Network Services Subsystem for querying for geocasting information.
3.2.1.3.2.4 The Core2Core Subsystem shall interface with the Service Monitor Subsystem for status information.
3.2.1.3.2.5 The Core2Core Subsystem shall interface with the User Permissions Subsystem querying for user permissions.
3.2.1.3.2.6 The Core2Core Subsystem shall interface with the User Security Subsystem to manage trust credentials.

3.2.1.4 Data Requirements

3.2.1.4.1 The Core2Core Subsystem shall maintain a knowledge base of data available with interfacing Core Systems.
3.2.1.4.2 The Core2Core Subsystem shall maintain a knowledge base of services available with interfacing Core Systems.
3.2.1.4.3 The Core2Core Subsystem shall maintain storage information to identify the interfacing Core System to which data can be forwarded.
3.2.1.4.4 The Core2Core Subsystem shall store geographic boundary coverage characteristics for services that are available.

3.2.2 Data Distribution Subsystem

The Data Distribution Subsystem maintains a directory of System Users that want data and facilitates the delivery of that data to those users. It supports multiple distribution mechanisms, including:

- Source-to-Points: The data provider communicates data directly to data consumers. In this case no data is sent to the Core System, however the Core is involved to check System User Permissions and to provide addressing services through those subsystems
- Publish-Subscribe: The data provider communicates data to the Data Distribution subsystem, which forwards it to all users that are subscribed to receive the data.

Data Distribution allows data consumers to specify (and change the specification of) data they wish to receive using criteria including:

- Data type
- Data quality characteristics
- Data format requirements
- Geographic area
- Sampling rate
- Minimum and maximum frequency of data forwarding

Data Distribution maintains a registry of which data consumers get what data according to the criteria defined above. Data Distribution Publish-Subscribe does not store or buffer data beyond that which is necessary to complete publish-subscribe actions. If a given data consumer is unable to receive data that it has subscribed to because of a communications or other system failure, the data in question may be lost. The degree to which data distribution buffering accommodates connectivity failures will be up to the Core System deployment. Some Cores may offer "temporary storage" in this fashion.

Data Distribution repackages data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Data Distribution will also maintain source-to-points information. With this option, the data consumer will connect directly to the data provider with the address supplied by the Data Distribution subsystem. When connected, the data provider sends the data directly to each consumer bypassing the Core System.

Data Distribution does not share or exchange data with other Core Systems. System Users that want data from multiple Cores need to subscribe to each Core.

3.2.2.1 Functional Requirements

3.2.2.1.1	**Data Request Processing**
3.2.2.1.1.1	The Data Distribution Subsystem shall accept System User's requests for data that include parameters describing how often the data are to be provided.
3.2.2.1.1.2	The Data Distribution Subsystem shall accept System User's requests for data that include parameters describing the length of time the data are to be provided.

3.2.2.1.1.3 The Data Distribution Subsystem shall provide information to a catalog describing the type of data the data provider is sending.

3.2.2.1.1.4 The Data Distribution Subsystem shall provide information to a catalog describing the quality characteristics of the type of data the data provider is sending.

3.2.2.1.1.5 The Data Distribution Subsystem shall provide information to a catalog describing the data format for each type of data the data provider is sending.

3.2.2.1.1.6 The Data Distribution Subsystem shall provide information to a catalog describing the geographic location where the data was generated from that the data provider is sending.

3.2.2.1.1.7 The Data Distribution Subsystem shall provide information to a catalog describing the sampling rate of the data that the data provider is sending.

3.2.2.1.1.8 The Data Distribution Subsystem shall provide a catalog describing the frequency of data forwarding.

3.2.2.1.2 The Data Distribution Subsystem shall send data request to User Permissions Subsystem.

3.2.2.1.3 The Data Distribution Subsystem shall maintain a registry of data requests.

3.2.2.1.3.1 The Data Distribution Subsystem shall maintain a registry of the requesters for data from the Core System.

3.2.2.1.3.2 The Data Distribution Subsystem shall maintain a registry of the data requested by System Users.

3.2.2.1.4 The Data Distribution Subsystem shall acknowledge the System User's request if the data type requested for distribution matches the information in the data catalog.

3.2.2.1.5 The Data Distribution Subsystem shall reject the System User's request if the data type requested for distribution does not match any information in the catalog.

3.2.2.1.6 The Data Distribution Subsystem shall report misbehavior data requests to the Misbehavior Management Subsystem.

3.2.2.1.7 When in Restricted Mode, the Data Distribution Subsystem shall prioritize System User's requests to receive data.

3.2.2.1.8 Data Request Processing - Source-to-points

3.2.2.1.8.1 The Data Distribution Subsystem shall provide a data publisher's information in a catalog when that data is distributed as an external source-to-point (when not through the Core System).

3.2.2.1.9 Data Provision Processing

3.2.2.1.9.1 The Data Distribution Subsystem shall accept requests to publish data from System Users that include how often the data are to be provisioned.

3.2.2.1.10 The Data Distribution Subsystem shall accept requests to publish data from System Users that include the length of time the data are to be provisioned.

3.2.2.1.10.1 The Data Distribution Subsystem shall provide a catalog defining the data being provisioned.

3.2.2.1.10.2 The Data Distribution Subsystem shall provide a catalog describing the type of data to be provisioned.

3.2.2.1.10.3 The Data Distribution Subsystem shall provide a catalog describing the data quality characteristics of the data to be provisioned.

3.2.2.1.10.4 The Data Distribution Subsystem shall provide a catalog describing the data formats of the data to be provided.

3.2.2.1.10.5 The Data Distribution Subsystem shall provide a catalog describing the geographic location of where the data was generated.

3.2.2.1.10.6 The Data Distribution Subsystem shall provide a catalog describing the sampling rate at which the data was collected.

3.2.2.1.10.7 The Data Distribution Subsystem shall provide a catalog describing the frequency of data forwarding.

3.2.2.1.10.8 The Data Distribution Subsystem shall provide a catalog describing the geographic area over which the data should be broadcast.

3.2.2.1.10.9 The Data Distribution Subsystem shall repackage data by parsing incoming data to extract only that data that the subscriber requires.

3.2.2.1.10.10 The Data Distribution Subsystem shall repackage data by parsing incoming data to extract restricted data that the publisher does not want to be sent to the subscriber.

3.2.2.1.11 When in Restricted Mode, the Data Distribution Subsystem shall prioritize System User's requests to publish data.

3.2.2.1.12 The Data Distribution Subsystem shall send requests to User Permissions Subsystem.

3.2.2.1.13 The Data Distribution Subsystem shall maintain a registry of publishing data for System Users.

3.2.2.1.13.1 The Data Distribution Subsystem shall maintain a registry of data on publishers for the Core System User.

3.2.2.1.14 The Data Distribution Subsystem shall positively acknowledge the request to the System User if the data can be published.

3.2.2.1.15 The Data Distribution Subsystem shall inform the System User if the request to publish cannot be processed.

3.2.2.1.16 The Data Distribution Subsystem shall provide the address of the data publisher to send their data based on the supplied criteria when the Core System does not store the data itself.

3.2.2.1.17 The Data Distribution Subsystem shall send misbehavior data provisioning to the Misbehavior Management Subsystem.

3.2.2.1.18 The Data Distribution Subsystem shall identify rate of incoming messages exceeding a threshold rate [TBD] from a System User as misbehavior.

3.2.2.1.19 The Data Distribution Subsystem shall report data rate misbehavior to the Misbehavior Management Subsystem.

3.2.2.1.20 Data Distribution Configuration and Operator Interface

3.2.2.1.20.1 The Data Distribution Subsystem shall support an interface to an authorized System Operator for editing the Publisher/Subscriber configuration for the Data Distribution Subsystem supported services.

3.2.2.1.20.2 The Data Distribution Subsystem shall provide an authorized System Operator with the configuration of the Data Distribution Subsystem supported services.

3.2.2.1.20.3 The Data Distribution Subsystem shall support an interface to an authorized System Operator for configuring the data that will be provided by the Core System.

3.2.2.1.20.4 The Data Distribution Subsystem shall support an interface to an authorized System Operator for configuring the data that will be provided by reference to their publisher only.

3.2.2.1.20.5 The Data Distribution Subsystem shall provide the registry of data available to the Core2Core Subsystem for data to be distributed to System Users.

3.2.2.1.20.6 The Data Distribution Subsystem shall receive contact information from the Core2Core Subsystem to populate the registry of data available for distribution.

3.2.2.1.20.7 The Data Distribution Subsystem shall populate the registry of data available for distribution.

3.2.2.1.20.8 The Data Distribution Subsystem shall provide contact information to the Core2Core Subsystem for other Core Systems to receive, so they can populate their registry of data available from the originating Core System.

3.2.2.1.20.9 The Data Distribution Subsystem shall provide data description information to the Core2Core Subsystem for other Core Systems to receive, so they can populate their registry of data available from the originating Core System.

3.2.2.1.20.10 The Data Distribution Subsystem shall receive data description information from the Core2Core Subsystem to populate the registry of data available for distribution.

3.2.2.1.20.11 Data Distribution Configuration and Operator - Source-to-point

3.2.2.1.20.11.1 The Data Distribution Subsystem shall support an interface to an authorized System Operator for editing the source-to-point configuration for the Data Distribution Subsystem supported services.

3.2.2.1.21 Data Distribution Subsystem state management functions

3.2.2.1.21.1 The Data Distribution Subsystem shall send operational state transitions to the Service Monitor Subsystem.

3.2.2.1.21.2 The Data Distribution Subsystem shall transition to the requested state when commanded by an authorized System Operator.

3.2.2.1.21.3 The Data Distribution Subsystem shall transition to degraded mode of operations when a hardware failure within the Data Distribution Subsystem is detected.

3.2.2.1.21.4 When operating in normal operational mode, the Data Distribution Subsystem shall accept data distribution requests from System Users.

3.2.2.1.21.5 The Data Distribution Subsystem shall send status to the Service Monitor Subsystem.

3.2.2.1.21.6 The Data Distribution Subsystem shall transition to degraded mode of operations when a software failure within the Data Distribution Subsystem is detected.

3.2.2.1.21.7 The Data Distribution Subsystem shall accept data distribution requests from other Core Systems when operating in Restricted Mode.

3.2.2.1.21.8 The Data Distribution Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.2.1.22 Obtaining time

3.2.2.1.22.1 The Data Distribution Subsystem shall accept the time of day from the Time Subsystem.

3.2.2.2 Performance Requirements

3.2.2.2.1 The Data Distribution Subsystem shall buffer forwarding data with a latency no greater than 500ms[TBD].

3.2.2.3 Interface Requirements

3.2.2.3.1 Data Distribution External Interfaces

3.2.2.3.1.1 The Data Distribution Subsystem shall support an interface to System Users to provide contact information for data being provisioned.

3.2.2.3.1.2 The Data Distribution Subsystem shall support an interface to System Users to provide a catalog defining the data being provisioned.

3.2.2.3.1.3 The Data Distribution Subsystem shall support an interface to System Users for requests to receive data being provisioned.

3.2.2.3.2 Data Distribution Internal Interfaces

3.2.2.3.2.1 The Data Distribution Subsystem shall interface with the Core2Core Subsystem for sharing data provisioning information to a backup Core System.

3.2.2.3.2.2 The Data Distribution Subsystem shall interface with the Misbehavior Management Subsystem for misbehavior management.

3.2.2.3.2.3 The Data Distribution Subsystem shall interface with the Network Services Subsystem for querying for geocasting information.

3.2.2.3.2.4 The Data Distribution Subsystem shall interface with the Service Monitor Subsystem for status information.

3.2.2.3.2.5 The Data Distribution Subsystem shall interface with the User Permissions Subsystem querying for user permissions.

3.2.2.3.2.6 The Data Distribution Subsystem shall interface with the User Security Subsystem to manage trust credentials.

3.2.2.4 Data Requirements

3.2.2.4.1 The Data Distribution Subsystem shall maintain a registry containing the list of data providers.

3.2.2.4.2 The Data Distribution Subsystem shall maintain a registry of the data that has been made available for publication.

3.2.2.4.3 The Data Distribution Subsystem shall maintain a registry containing the list of data requesters.

3.2.2.4.4 The Data Distribution Subsystem shall maintain a registry of the data that have been requested.

3.2.2.4.5	The Data Distribution Subsystem shall maintain a registry of which data consumers receive what data according to the criteria provided by the requesters.
3.2.2.4.6	The Data Distribution Subsystem shall maintain a registry of publisher information including Data Types and Sources, Data Acceptance Changes, Data Acceptance or Discard, Data Type and Source, Permission, Data Type and Source Request, Existing Acceptance and/or Changes, Data Coverage Conflict, Data Acceptance Details.
3.2.2.4.7	The Data Distribution Subsystem shall maintain a registry of subscriber information including Data Type and Source Request, Existing Acceptance and/or Changes, Data Description, Subscription Details, Subscriber ID, Data Subscription Details, and Data Subscription Changes.

3.2.3 Misbehavior Management Subsystem

The Misbehavior Management Subsystem analyzes messages sent to the Core System to identify users operating outside of their assigned permissions. It works with the User Permissions subsystem to identify suspicious requests and to maintain a record of specifically identifiable users that:

1. Provide false or misleading data
2. Operate in such a fashion as to impede other users
3. Operate outside of their authorized scope

Because most end users will rarely interface with the Core System, Misbehavior Management will also accept reports of misbehaving users from other users. Center, Mobile, and Field users can send misbehavior reports that reference credentials attached to messages and note the type of misbehavior in question. Misbehavior Management will record such reports and according to a set of Core System Personnel-controlled rules will determine when to revoke credentials from such reported misbehaving users. For anonymous users revocation is more complex and may result instead in a lack of credential renewal. Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

3.2.3.1 Functional Requirements

3.2.3.1.1	The Misbehavior Management Subsystem shall receive Denial of Service (DoS) attack reports on the Core System from other subsystems in the Core System.
3.2.3.1.2	**Misbehavior Reporting**
3.2.3.1.2.1	The Misbehavior Management Subsystem shall accept reports of System User misbehavior by other System Users.
3.2.3.1.2.2	The Misbehavior Management Subsystem shall support an interface to an authorized System Operator for creating a misbehavior entry for a System User.
3.2.3.1.2.3	The Misbehavior Management Subsystem shall support the configuration for operator login failure attempts allowed before considered a misbehavior.
3.2.3.1.3	**Core System Access Control**
3.2.3.1.3.1	The Misbehavior Management Subsystem shall record unauthorized operator access attempts to Core System Services to an unauthorized service access log.
3.2.3.1.3.2	The Misbehavior Management Subsystem shall record unauthorized operator login attempts to an unauthorized login log.

3.2.3.1.3.3 The Misbehavior Management Subsystem shall provide logs of unauthorized login attempts to an authorized System Operator.

3.2.3.1.3.4 The Misbehavior Management Subsystem shall provide logs of unauthorized service access records to an authorized System Operator.

3.2.3.1.3.5 The Misbehavior Management Subsystem shall record System User misbehavior reports in a System User misbehavior log.

3.2.3.1.3.6 The Misbehavior Management Subsystem shall provide System User misbehavior logs to an authorized System Operator upon request.

3.2.3.1.3.7 The Misbehavior Management Subsystem shall provide System User misbehavior record reports to an authorized System Operator upon occurrence.

3.2.3.1.3.8 When in Restricted Mode, the Misbehavior Management Subsystem shall prioritize misbehavior reporting.

3.2.3.1.4 Misbehavior Management Subsystem state management functions

3.2.3.1.4.1 The Misbehavior Management Subsystem shall send operational state transitions to the Service Monitor Subsystem.

3.2.3.1.4.2 The Misbehavior Management Subsystem shall transition to the requested state when commanded by an authorized System Operator.

3.2.3.1.4.3 The Misbehavior Management Subsystem shall transition to degraded mode of operations when a hardware failure within the Misbehavior Management Subsystem is detected.

3.2.3.1.4.4 When operating in normal operational mode, the Misbehavior Management Subsystem shall accept System User Misbehavior reports from System Users.

3.2.3.1.4.5 The Misbehavior Management Subsystem shall send status to the Service Monitor Subsystem.

3.2.3.1.4.6 The Misbehavior Management Subsystem shall transition to degraded mode of operations when a software failure within the Misbehavior Management Subsystem is detected.

3.2.3.1.4.7 The Misbehavior Management Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.3.1.5 Misbehavior Post Processing functions

3.2.3.1.5.1 The Misbehavior Management Subsystem shall correlate the misbehavior reports received from System Users.

3.2.3.1.5.2 The Misbehavior Management Subsystem shall generate a report that identifies misbehaving System Users.

3.2.3.1.5.2.1 The Misbehavior Management Subsystem shall send the report of misbehaving System Users to the User Permissions Subsystem.

3.2.3.1.5.2.2 The Misbehavior Management Subsystem shall send the report of misbehaving System Users to the User Security Subsystem.

3.2.3.1.5.3 The Misbehavior Management Subsystem shall support configuration of correlation parameters by an authorized operator.

3.2.3.1.5.4 The Misbehavior Management Subsystem shall accept input from an authorized System Operator to initiate correlation processing.

3.2.3.1.5.5 The Misbehavior Management Subsystem shall store information regarding misbehavior reports from other Core System subsystems.

3.2.3.1.6 Obtaining time

3.2.3.1.6.1 The Misbehavior Management Subsystem shall accept the time of day from the Time Subsystem

3.2.3.2 Performance Requirements

3.2.3.2.1 The Misbehavior Management Subsystem shall process up to [TBD] misbehavior reports per minute from System Users.

3.2.3.2.2 The Misbehavior Management Subsystem shall perform the misbehavior report correlation processing [TBD] times per hour.

3.2.3.2.3 The Misbehavior Management Subsystem shall provide storage to securely store [TBD] misbehavior reports.

3.2.3.3 Interface Requirements

3.2.3.3.1 Misbehavior Management External Interfaces

3.2.3.3.1.1 The Misbehavior Management Subsystem shall support an interface for the System Users to send misbehavior reports regarding other System Users.

3.2.3.3.1.2 The Misbehavior Management Subsystem on a Core System shall support an interface for other Core Systems to send misbehavior reports regarding System Users.

3.2.3.3.1.3 The Misbehavior Management Subsystem shall support an interface for the System Users to report denial-of-service (DoS) attacks.

3.2.3.3.2 Misbehavior Management Internal Interfaces

3.2.3.3.2.1 The Misbehavior Management Subsystem shall interface with the Core2Core Subsystem for sharing data provisioning information to a backup Core System.

3.2.3.3.2.2 The Misbehavior Management Subsystem shall interface with the Service Monitor Subsystem for status information.

3.2.3.3.2.3 The Misbehavior Management Subsystem shall interface with the User Permissions Subsystem querying for user permissions.

3.2.3.3.2.4 The Misbehavior Management Subsystem shall interface with the User Security Subsystem to manage trust credentials.

3.2.3.4 Data Requirements

3.2.3.4.1 The Misbehavior Management Subsystem shall maintain a history of System Users misbehavior reports.

3.2.3.4.2 The Misbehavior Management Subsystem shall maintain a history of System Users who have misbehaved.

3.2.3.4.3 The Misbehavior Management Subsystem shall maintain a registry of data for unauthorized login attempts.

3.2.3.4.4 The Misbehavior Management Subsystem shall maintain a registry of usernames for failed login attempt.

3.2.3.4.5 The Misbehavior Management Subsystem shall maintain a registry of time for when a failed login attempt occurred.

3.2.3.4.6 The Misbehavior Management Subsystem history of data shall be stored for a configurable length of time.

3.2.4 Network Services Subsystem

The Network Services Subsystem provides information to System Users and Core System services that enable communication between those users and services. The Network Services subsystem will provide the information necessary for users to communicate with other users that have given permission to be communicated with. Network Services will also provide the information necessary to enable users to communicate with a group of users by maintaining information regarding available communications methods, addresses, and performance characteristics for geo-cast communications.

Network Services will also provide management for Communications Layer resources. It will enable decisions about which communications medium to use when more than one is available. This includes identifying available communications methods current performance characteristics and applicable user permission levels. Permission requirements will be coordinated with the User Permissions subsystem.

3.2.4.1 Functional Requirements

3.2.4.1.1	**Geocasting Service**
3.2.4.1.1.1	The Network Services Subsystem Geocasting Service (GCS) shall support IP version 6 as the network protocol.
3.2.4.1.1.2	The Network Services Subsystem GCS shall verify the credentials of the sender before registering the sender of the geocast information.
3.2.4.1.1.3	The Network Services Subsystem GCS shall verify with the User Permission Subsystem that the sender has sufficient privilege to send the message using the geocast service.
3.2.4.1.1.4	The Network Services Subsystem GCS shall discard the message submitted for geocast when the message fails integrity check.
3.2.4.1.1.5	The Network Services Subsystem GCS shall discard the message submitted for geocast when the message frequency exceeds the configured limit.
3.2.4.1.1.6	The Network Services Subsystem GCS shall report geocast sender misbehavior to the Misbehavior Management Subsystem.
3.2.4.1.1.7	The Network Services Subsystem GCS shall support an interface to the System Operator to configure the geocast areas using latitude and longitude coordinates.
3.2.4.1.1.8	The Network Services Subsystem shall accept a request from a System User to provide data to a specified geographic area.
3.2.4.1.1.9	The Network Services Subsystem shall send a response to a System User's request to allow data to be sent to a specified geographic area.
3.2.4.1.2	**System Operator interface, logging and retrieval**
3.2.4.1.2.1	The Network Services Subsystem shall support an interface to an authorized System Operator for creating configuration for its supported services.
3.2.4.1.2.2	The Network Services Subsystem shall support an interface to an authorized System Operator for viewing the configuration for all its supported services.
3.2.4.1.2.3	The Network Services Subsystem GCS shall record in the system log when a message meant for geocast is discarded.
3.2.4.1.3	**Network Services Subsystem state management functions**
3.2.4.1.3.1	When operating in normal operational mode, the Network Services Subsystem shall accept registration requests for geocast from System Users.
3.2.4.1.3.2	The Network Services Subsystem shall send status to the Service Monitor Subsystem.
3.2.4.1.3.3	The Network Services Subsystem shall transition to degraded mode of operations when a software failure within the Network Service Subsystem is detected.
3.2.4.1.3.4	The Network Services Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.
3.2.4.1.3.5	The Network Services Subsystem shall send operational state transitions to the Service Monitor Subsystem.
3.2.4.1.3.6	The Network Services Subsystem shall transition to the requested state when commanded by an authorized System Operator.
3.2.4.1.3.7	The Network Services Subsystem shall transition to degraded mode of operations when a hardware failure within the Network Services Subsystem is detected.

3.2.4.1.3.8 When operating in normal operational mode, the Network Services Subsystem shall accept requests for geocast from System Users.

3.2.4.1.3.9 Network Services Subsystem misbehavior reporting

3.2.4.1.3.10 The Network Services Subsystem shall report data request misbehavior to the Misbehavior Management Subsystem.

3.2.4.1.3.11 The Network Services Subsystem shall report data routing misbehavior to the Misbehavior Management Subsystem.

3.2.4.1.3.12 The Network Services Subsystem shall report data intrusion misbehavior to the Misbehavior Management Subsystem.

3.2.4.1.3.13 The Network Services Subsystem shall report data detection misbehavior to the Misbehavior Management Subsystem.

3.2.4.1.3.14 The Network Services Subsystem shall report Internet connectivity misbehavior to the Misbehavior Management Subsystem.

3.2.4.1.4 Obtaining time

3.2.4.1.4.1 The Network Services Subsystem shall accept the time of day from Time Subsystem.

3.2.4.2 Performance Requirements

3.2.4.2.1 The Network Services Subsystem GCS shall support up to [TBD] geocast sessions at any given time.

3.2.4.2.2 The Network Services Subsystem GCS shall support up to [TBD] megabits per second (Mbps) per geocast stream.

3.2.4.3 Interface Requirements

3.2.4.3.1 Network Services External Interfaces

3.2.4.3.1.1 The Network Services Subsystem GCS shall support an interface to the System User for registering to request Core System to geocast messages.

3.2.4.3.1.2 The Network Services Subsystem GCS shall support an interface to the System Operator to configure a limit on the frequency of geocast transmission from an individual sender.

3.2.4.3.1.3 The Network Services Subsystem shall support an interface to an authorized System Operator to configure system network parameters.

3.2.4.3.1.4 The Network Services Subsystem shall support an Internet interface to connect to System Users

3.2.4.3.2 Network Services Internal Interfaces

3.2.4.3.2.1 The Network Services Subsystem shall interface with the Core2Core Subsystem for sharing data provisioning information to a backup Core System.

3.2.4.3.2.2 The Network Services Subsystem shall interface with the Data Distribution System Services Subsystem for querying for geocasting information.

3.2.4.3.2.3 The Network Services Subsystem shall interface with the Misbehavior Management Subsystem for misbehavior management.

3.2.4.3.2.4 The Network Services Subsystem shall interface with the Service Monitor Subsystem for status information.

3.2.4.3.2.5 The Network Services Subsystem shall interface with the User Permissions Subsystem querying for user permissions.

3.2.4.3.2.6 The Network Services Subsystem shall interface with the User Security Subsystem to manage trust credentials.

3.2.4.4 Data Requirements

3.2.4.4.1 The Network Services Subsystem shall store configurable geocast area information, including latitude and longitude coordinates.

3.2.5 Service Monitor Subsystem

The Service Monitor Subsystem monitors the status of Core System services, interfaces, and communications networks connected to the Core. It informs System Users of the availability and status of its services.

Service Monitor also monitors the integrity of internal Core System components and supporting software, and mitigates against vulnerabilities. This includes periodic verification of the authenticity of Core service software and supporting software. This also includes monitoring for vulnerabilities including but not limited to virus protection, network port monitoring, and monitoring for patches to third party components. Should a vulnerability be detected or a component of the Core found to have lost integrity, Service Monitor takes steps to mitigate against damage and performance degradation.

The Service Monitor Subsystem ensures the physical security of Core System services by monitoring the environmental conditions that Core components operate in (e.g. temperature and humidity) as well as the condition of its power system. It takes steps to mitigate against system failures in the event that environmental conditions exceed operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of Core service operations, as well as Core System Personnel (Core System staff) notification.

Service Monitor also monitors the performance of all services and interfaces and makes performance metrics available to Core System Personnel (Core System staff).

3.2.5.1 Functional Requirements

3.2.5.1.1	The Service Monitor Subsystem shall accept status from subsystems within the Core System.
3.2.5.1.1.1	The Service Monitor Subsystem shall report status when hardware is available.
3.2.5.1.1.2	The Service Monitor Subsystem shall report status when hardware has degraded.
3.2.5.1.1.3	The Service Monitor Subsystem shall report status when hardware has failed.
3.2.5.1.1.4	The Service Monitor Subsystem shall report CPU performance status from each Core System node to the System Operator.
3.2.5.1.1.5	The Service Monitor Subsystem shall report I/O data performance status from each Core System node to the System Operator.
3.2.5.1.1.6	The Service Monitor Subsystem shall report status to an authorized System Operator.
3.2.5.1.1.7	The Service Monitor Subsystem shall store report status to a status history log.
3.2.5.1.1.8	The Service Monitor Subsystem shall accept failed software status from the Core System subsystems.
3.2.5.1.1.9	The Service Monitor Subsystem shall accept degraded software status from the Core System subsystems.
3.2.5.1.1.10	The Service Monitor Subsystem shall accept operational software status from the Core System subsystems.
3.2.5.1.1.11	The Service Monitor Subsystem shall accept failed hardware status from the Core System subsystems.
3.2.5.1.1.12	The Service Monitor Subsystem shall accept degraded hardware status from the Core System subsystems.

3.2.5.1.1.13	The Service Monitor Subsystem shall accept operational hardware status from the Core System subsystems.
3.2.5.1.1.14	The Service Monitor Subsystem shall accept an authorized operator command to change States.
3.2.5.1.1.15	The Service Monitor Subsystem shall accept an authorized operator command to change to Restricted Mode.
3.2.5.1.1.16	The Service Monitor Subsystem shall accept an authorized operator command to change to Operational Mode.
3.2.5.1.1.17	The Service Monitor Subsystem shall detect malicious software running within the Core System.
3.2.5.1.1.18	The Service Monitor Subsystem shall notify an authorized System Operator when malicious software has been detected within the Core System.
3.2.5.1.2	The Service Monitor Subsystem shall send a list of Core System Service states to System Users upon a state transition.
3.2.5.1.3	The Service Monitor Subsystem shall send a list of Core System Service states to a System User upon request.
3.2.5.1.4	The Service Monitor Subsystem shall send a list of Core System Service statuses from other Core System locations to a system user upon request.
3.2.5.1.5	The Service Monitor Subsystem shall send a list of Core System services that are available from other Core Systems when that service is degraded on the local Core System.
3.2.5.1.6	The Service Monitor Subsystem shall send a list of Core System services that are available from other Core Systems when that service has failed on the local Core System.
3.2.5.1.7	The Service Monitor Subsystem shall accept System User's requests for a list of available Core System services.
3.2.5.1.8	The Service Monitor Subsystem shall perform health checks in the Core System while in the operational state upon request from an authorized System Operator
3.2.5.1.8.1	The Service Monitor Subsystem shall send the results of an internal health check to the System Operator upon request.
3.2.5.1.9	The Service Monitor Subsystem shall implement mechanisms to recover degraded Core System services in the Core System.
3.2.5.1.10	The Service Monitor Subsystem shall implement mechanisms to recover failed Core System services in the Core System.
3.2.5.1.11	The Service Monitor Subsystem shall verify the authenticity of every software update.
3.2.5.1.11.1	The Service Monitor Subsystem shall display software status to an authorized System Operator upon request.
3.2.5.1.11.2	The Service Monitor Subsystem shall install only software updates that have been authenticated.
3.2.5.1.11.3	The Service Monitor Subsystem shall store the versions of the installed software.
3.2.5.1.11.4	The Service Monitor Subsystem shall reject a software update when authenticity has failed verification.
3.2.5.1.11.5	The Service Monitor Subsystem shall send an alert to an authorized System Operator upon rejecting a software update.
3.2.5.1.11.6	The Service Monitor Subsystem shall provide the history of software updates when requested by an authorized System Operator.
3.2.5.1.11.7	The Service Monitor Subsystem shall provide the history of software updates to the System Operator that includes version numbers of the software installed.
3.2.5.1.11.8	The Service Monitor Subsystem shall provide the history of software updates to the System Operator that includes timestamps that the software installation occurred.
3.2.5.1.11.9	The Service Monitor Subsystem shall provide the version of the software that is currently running in the Core System.
3.2.5.1.11.10	The Service Monitor Subsystem shall maintain an audit log on the installation of software updates.
3.2.5.1.11.11	The Service Monitor Subsystem shall support an interface to an authorized System Operator for configuring parameters that control the software configuration.

3.2.5.1.11.12 The Service Monitor Subsystem shall maintain an audit log on the installation of hardware updates.

3.2.5.1.12 The Service Monitor Subsystem shall support an interface to an authorized System Operator for modifying hardware configuration parameters.

3.2.5.1.12.1 The Service Monitor Subsystem shall upgrade hardware components by an authorized System Operator upon request.

3.2.5.1.12.2 The Service Monitor Subsystem shall add hardware components by an authorized System Operator upon request

3.2.5.1.12.3 The Service Monitor Subsystem shall reduce hardware components no longer needed by an authorized System Operator upon request.

3.2.5.1.12.4 The Service Monitor Subsystem shall identify hardware configuration components upon request from an authorized System Operator.

3.2.5.1.12.5 The Service Monitor Subsystem shall display hardware status to an authorized System Operator.

3.2.5.1.13 The Service Monitor Subsystem shall accept state transitions from other Core System subsystems.

3.2.5.1.14 The Service Monitor Subsystem shall transition to the requested state when requested by an authorized System Operator.

3.2.5.1.15 The Service Monitor Subsystem shall accept state transition changes from subsystems within the Core System.

3.2.5.1.16 The Service Monitor Subsystem shall transition to degraded mode of operations when a hardware failure within the Service Monitor Subsystem is detected

3.2.5.1.17 When operating in normal operational mode, the Service Monitor Subsystem shall send a list of Core System Services to other Core System locations.

3.2.5.1.18 When operating in normal operational mode, the Service Monitor Subsystem shall send a list of Core System Services to System Users.

3.2.5.1.19 The Service Monitor Subsystem shall report a recommended failover, when failover conditions exist, to an authorized System Operator when another Core System is available.

3.2.5.1.20 The Service Monitor Subsystem shall transition to degraded mode of operations when a software failure within the Service Monitor Subsystem is detected.

3.2.5.1.21 The Service Monitor Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.5.1.22 The Service Monitor Subsystem shall accept the time of day from the Time Subsystem.

3.2.5.2 Performance Requirements

3.2.5.2.1 The Service Monitor Subsystem shall notify an authorized System Operator within 30 seconds upon a software component failure.

3.2.5.2.2 The Service Monitor Subsystem shall notify an authorized System Operator within 30 seconds upon a hardware component failure.

3.2.5.2.3 The Service Monitor Subsystem shall notify an authorized System Operator within 30 seconds upon a connectivity interface failure.

3.2.5.2.4 The Service Monitor Subsystem shall send a list of Core System Service states to a System User every 15 minutes.

3.2.5.2.5 The Service Monitor Subsystem shall send an error report to an authorized System Operator when a periodically operational state message from a Core System subsystem is not received after 1500ms[TBD].

3.2.5.3 Interface Requirements

3.2.5.3.1 Service Monitor External Requirements

3.2.5.3.1.1 The Service Monitor Subsystem shall support an interface to send a list of Core System Service states to System Users.

3.2.5.3.1.2 The Service Monitor Subsystem shall support an interface to send a list of Core System Service states upon System Users request.

3.2.5.3.1.3 The Service Monitor Subsystem shall interface to an authorized System Operator.

3.2.5.3.2 Service Monitor Internal Requirements

3.2.5.3.2.1 The Service Monitor Subsystem shall interface with the Core2Core Subsystem for sharing Core System status information to a backup Core System.

3.2.5.4 Data Requirements

3.2.5.4.2 The Service Monitor Subsystem shall store other interfacing Core System states.

3.2.5.4.3 The Service Monitor Subsystem shall store subsystem states from the Core System subsystem.

3.2.5.4.4 The Service Monitor Subsystem shall store subsystem states from other interfacing Core Systems.

3.2.5.4.5 The Service Monitor Subsystem shall store the service status from the Core System.

3.2.5.4.6 The Service Monitor Subsystem shall store the service status from other interfacing Core Systems.

3.2.6 Time Subsystem

The Time Subsystem uses a time base available to all System Users and makes this time available to all Core System services which use this time base whenever a time reference is required.

3.2.6.1 Functional Requirements

3.2.6.1.1 The Time Subsystem shall receive time synchronization data from an external reference time source.

3.2.6.1.2 The Time Subsystem shall send time to all Core System subsystems every 100ms [TBD].

3.2.6.1.3 The Time Subsystem shall record time synchronization anomalies in a log.

3.2.6.1.4 The Time Subsystem shall provide time status anomalies to an authorized System Operator concerning time synchronization anomalies.

3.2.6.1.5 The Time Subsystem shall provide Universal Time, Coordinated (UTC) time to Core System subsystems. Note: UTC is also known as Zulu time.

3.2.6.1.6 The Time Subsystem shall transition to degraded mode of operations when a hardware failure within the Time Subsystem is detected.

3.2.6.1.7 The Time Subsystem shall transition to degraded mode of operations when a software failure within the Time Subsystem is detected.

3.2.6.1.8 The Time Subsystem shall transition to degraded mode of operations when a software failure within the User Security Subsystem is detected.

3.2.6.1.9 The Time Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.6.1.10 The Time Subsystem shall transition to the requested state when commanded by an authorized System Operator.

3.2.6.1.11 The Time Subsystem shall provide synchronization time to other Core System subsystems when operating in normal operational mode.

3.2.6.1.12 The Time Subsystem shall provide synchronization time to other Core System subsystems when operating in Restricted Mode.

3.2.6.2 Performance Requirements

3.2.6.2.1 The time of day shall not drift (lagging or leading in time) from the external time source standard time reference by more than [TBD] 1 second per year.

3.2.6.2.2 The Time Subsystem shall synchronize the time of day with all the Core Subsystems every 10ms (TBD).

3.2.6.3 Interface Requirements

3.2.6.3.1 Time External Interfaces

3.2.6.3.1.1 The Time Subsystem shall support an interface to the National Institute of Standards and Technology (NIST).

3.2.6.3.1.2 The Time Subsystem shall support an interface via the Core2Core Subsystem to send time to other Core Systems.

3.2.6.3.2 Time Internal Interfaces

3.2.6.3.2.1 The Time Subsystem shall interface with the Core2Core Subsystem to supply time of day.

3.2.6.3.2.2 The Time Subsystem shall interface with the Data Distribution Subsystem for sharing data provisioning information to a backup Core System.

3.2.6.3.2.3 The Time Subsystem shall interface with the Misbehavior Management Subsystem to supply time of day.

3.2.6.3.2.4 The Time Subsystem shall interface with the Network Services Subsystem to supply time of day.

3.2.6.3.2.5 The Time Subsystem shall interface with the Service Monitor Subsystem to supply time of day.

3.2.6.3.2.6 The Time Subsystem shall interface with the User Permissions Subsystem to supply time of day.

3.2.6.3.2.7 The Time Subsystem shall interface with the User Security Subsystem to supply time of day.

3.2.6.4 Data Requirements

None.

3.2.7 User Permissions Subsystem

The User Permissions Subsystem provides tools allowing System Users to verify whether a given user, identified by digital certificate-based credentials, is authorized to request or perform the action requested in the message payload. It also maintains the status of users, whether they have a specific account, their allowed behaviors with defined permissions (publish, subscribe, actions allowed to request, and administration etc.), or if they belong to an anonymous group. User Permissions provides the tools for Core System Personnel to: create new users and groups, modify existing users and groups, and modify permissions associated with users and groups.

3.2.7.1 Functional Requirements

3.2.7.1.1 Managing Core System Personnel User Information and Permissions

3.2.7.1.1.1 The User Permissions Subsystem shall support an interface to Core System Personnel for performing authorized Core System management operations based on their user permissions.

3.2.7.1.1.2 The User Permissions Subsystem shall prohibit Core System Personnel from performing unauthorized Core System Management operations based on their user permissions.

3.2.7.1.1.3 The User Permissions Subsystem shall provide Core System Personnel registration information to other Core System subsystems.

3.2.7.1.1.4 The User Permissions Subsystem shall provide Core System Personnel user permissions information to other Core System subsystems.

3.2.7.1.2 Managing System User Information and Permissions

3.2.7.1.2.1 The User Permissions Subsystem shall compare the System User's certificate(s) with the Certificate Revocation List provided by the User Security Subsystem.

3.2.7.1.2.2 The User Permissions Subsystem shall allow a System User to perform authorized system operations, based on their permissions.

3.2.7.1.2.3 The User Permissions Subsystem shall record when a System User performs an authorized system user operation.

3.2.7.1.2.4 The User Permissions Subsystem shall prohibit a System User from performing unauthorized system user operations based on their user permissions.

3.2.7.1.2.5 The User Permissions Subsystem shall record when a System User is restricted from performing an unauthorized system user operation based on their user permissions.

3.2.7.1.2.6 The User Permissions Subsystem shall provide System User registration with user permissions information to other Core System subsystems.

3.2.7.1.2.7 The User Permissions Subsystem shall report unauthorized operator login attempts to the Misbehavior Management Subsystem.

3.2.7.1.2.8 The User Permissions Subsystem shall report unauthorized operator access attempts to the Misbehavior Management Subsystem.

3.2.7.1.2.9 The User Permissions Subsystem shall report unauthorized System User access attempts to the Misbehavior Management Subsystem.

3.2.7.1.2.10 The User Permissions Subsystem shall determine the registration characteristics of the System User based on the System User's certificate(s).

3.2.7.1.2.11 The User Permissions Subsystem shall transition to degraded mode of operations when a hardware failure within the User Permissions Subsystem is detected.

3.2.7.1.2.12 The User Permissions Subsystem shall transition to degraded mode of operations when a software failure within the User Permissions Subsystem is detected.

3.2.7.1.2.13 The User Permissions Subsystem shall transition to the requested mode of operation when commanded by an authorized System Operator.

3.2.7.1.2.14 The User Permissions Subsystem shall transition to the requested state when commanded by an authorized System Operator.

3.2.7.1.3 Obtaining time

3.2.7.1.3.1 The User Permissions Subsystem shall accept the time of day from the Time Subsystem.

3.2.7.2 Performance Requirements

3.2.7.2.1 Upon request, the User Permissions Subsystem shall provide Core System Personnel registration information to other Core System subsystems with [TBD] seconds.

3.2.7.2.2 Upon request, the User Permissions Subsystem shall provide Core System Personnel user permissions information to other Core System subsystems with [TBD] seconds.

3.2.7.2.3 Upon request from an authorized System Operator, the User Permissions Subsystem shall provide System User registration information to other Core System subsystems within [TBD] seconds.

3.2.7.2.4 Upon request from an authorized System Operator, the User Permissions Subsystem shall provide System User permissions information to other Core System subsystems within [TBD] seconds.

3.2.7.3 Interface Requirements

3.2.7.3.1 User Permissions External Interfaces

3.2.7.3.1.1 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to register Core System Personnel.

3.2.7.3.1.1.1 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the Core System Personnel user type (Administrator, Operator, Maintainer, Developer or Deployer).

3.2.7.3.1.1.2 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the Core System Personnel user identification (Name and Contact Information).

3.2.7.3.1.1.3 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the Core System Personnel home location.

3.2.7.3.1.1.4 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the Core System Personnel user permissions.

3.2.7.3.1.2 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to register a System User.

3.2.7.3.1.2.1 The User Permissions Subsystem shall accept certificate(s) from a System User.

3.2.7.3.1.2.2 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User identification (Name and Contact Information or Anonymous) for a valid system user certificate.

3.2.7.3.1.2.3 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User role(s) [TBD] for a valid system user certificate.

3.2.7.3.1.2.4 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User responsibilities [TBD] for a valid system user certificate.

3.2.7.3.1.2.5 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User location if fixed for a valid system user certificate.

3.2.7.3.1.2.6 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User's home Core System for a valid system user certificate.

3.2.7.3.1.2.7 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User's status [TBD] for a valid system user certificate.

3.2.7.3.1.2.8 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the System User's user permissions [TBD] for a valid system user certificate.

3.2.7.3.1.3 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to register another Core System.

3.2.7.3.1.3.1 The User Permissions Subsystem shall accept certificate(s) from another Core System.

3.2.7.3.1.3.2 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify another Core System's identification (Name and Contact Information) for a valid Core System certificate.

3.2.7.3.1.3.3 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System role(s) [TBD] for a valid Core System certificate.

3.2.7.3.1.3.4 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's responsibilities [TBD] for a valid Core System certificate.

3.2.7.3.1.3.5 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's location for a valid Core System certificate.

3.2.7.3.1.3.6 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's region of responsibility for a valid Core System certificate.

3.2.7.3.1.3.7 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's available services for a valid Core System certificate.

3.2.7.3.1.3.8 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's status [TBD] for a valid Core System certificate.

3.2.7.3.1.3.9 The User Permissions Subsystem shall support an interface to an authorized Core System Administrator to modify the other Core System's user permissions [TBD] for a valid Core System certificate.

3.2.7.3.1.4 The User Permissions Subsystem shall send User Permission data to other Core Systems.

3.2.7.3.1.4.1 The User Permissions Subsystem shall request authorized System User registration information from other Core Systems.

3.2.7.3.1.4.2 The User Permissions Subsystem shall request authorized System User permissions information from other Core Systems.

3.2.7.3.1.4.3 The User Permission Subsystem shall receive authorized System User registration information from other Core Systems.

3.2.7.3.1.4.4 The User Permission Subsystem shall receive authorized System User permissions information from other Core Systems.

3.2.7.3.2 User Permissions Internal Interfaces

3.2.7.3.2.1 The User Permissions Subsystem shall interface with the Core2Core Subsystem to provide permission verification.

3.2.7.3.2.2 The User Permission Subsystem shall interface with the Data Distribution Subsystem for sharing data provisioning information to a backup Core System.

3.2.7.3.2.3 The User Permissions Subsystem shall interface with the Misbehavior Management Subsystem to provide permission verification.

3.2.7.3.2.4 The User Permissions Subsystem shall interface with the Network Services Subsystem to provide permission verification.

3.2.7.3.2.5 The User Permissions Subsystem shall interface with the Service Monitor Subsystem to provide permission verification.

3.2.7.3.2.6 The User Permissions Subsystem shall interface with the User Security Subsystem to provide permission verification.

3.2.7.4 Data Requirements

3.2.7.4.1 The User Permissions Subsystem shall store the Core System Personnel registration information.

3.2.7.4.2 The User Permissions Subsystem shall store the Core System Personnel user permission information.

3.2.7.4.3 The User Permissions Subsystem shall store the System User registration information.

3.2.7.4.4 The User Permissions Subsystem shall store the System User permission information.

3.2.7.4.5 The User Permissions Subsystem shall store other Core System registration information.

3.2.7.4.6 The User Permissions Subsystem shall store the other Core System user permission information.

3.2.7.4.7 The User Permissions Subsystem shall store the System User's provider user permission information.

3.2.8 User Security Subsystem

The User Security Subsystem manages access rules and credentials in the form of digital certificates (including X.509, 1609.2 identity. and 1609.2 anonymous certificates) for all System Users and Core System components that require and are entitled to them. It creates and distributes cryptographic keys to qualifying System Users. It works with User Permissions to determine whether a given user applying for credentials or keys is entitled to them. It also manages the revocation of credentials and the distribution of Certificate Revocation Lists (CRLs) of disallowed credentials to interested System Users. User Security may use an External Support System to manage certificates, but such a determination is a design decision and will be deferred until the system architecture is defined.

3.2.8.1 Functional Requirements

3.2.8.1.1 Message Authentication and Confidentiality

3.2.8.1.1.1 The User Security Subsystem shall receive certificate request messages for 1609.2 Anonymous Certificates from System Users.

3.2.8.1.1.2 The User Security Subsystem shall verify signed messages received from the System Users.

3.2.8.1.1.3 The User Security Subsystem shall decrypt encrypted messages received from System Users.

3.2.8.1.1.4 The User Security Subsystem shall decrypt encrypted messages received from configured external Certification Authorities.

3.2.8.1.1.5 The User Security Subsystem shall verify signed messages received from configured external Certification Authorities.

3.2.8.1.1.6 The User Security Subsystem shall encrypt messages to System Users when an encrypted message originates from the Core System.

3.2.8.1.1.7 The User Security Subsystem shall sign messages to System Users when a signed message originates from the Core System.

3.2.8.1.1.8 The User Security Subsystem shall encrypt messages to other Core Systems.

3.2.8.1.1.9 The User Security Subsystem shall sign messages to other Core Systems.

3.2.8.1.1.10 The User Security Subsystem shall encrypt messages to configured external Certification Authorities (CA) when the CA is external to the Core System.

3.2.8.1.1.11 The User Security Subsystem shall sign messages to configured external Certification Authorities (CA) when the CA is external to the Core System.

3.2.8.1.1.12 The User Security Subsystem shall discard messages from System Users which fail message Integrity checks.

3.2.8.1.1.13 The User Security Subsystem shall discard messages from other Core Systems which fail message Integrity checks.

3.2.8.1.1.14 The User Security Subsystem shall manage a persistent connection to other interfacing Core Systems.

3.2.8.1.1.15 The User Security Subsystem shall send misbehavior information to the Misbehavior Management Subsystem when a signed message cannot be validated from a System User.

3.2.8.1.2 1609.2 Certificate Authority Functions

3.2.8.1.2.1 The User Security Subsystem shall support IEEE 1609.2 Certificate Authority functions to System Users as defined in IEEE 1609.2 specification.

3.2.8.1.2.2 The User Security Subsystem shall support issuance of 1609.2 Anonymous certificates to System Users as defined in IEEE 1609.2 specification.

3.2.8.1.2.3 The User Security Subsystem shall support issuance of 1609.2 Identity certificates to System Users as defined in IEEE 1609.2 specification.

3.2.8.1.2.4 The User Security Subsystem shall provide secure storage for 1609.2 CA private keys.

3.2.8.1.2.5 The User Security Subsystem shall provide secure storage for IEEE 1609.2 root and System User certificates.

3.2.8.1.2.6 The User Security Subsystem shall provide secure storage for IEEE 1609.2 Certificate Revocation Lists (CRL).

3.2.8.1.2.7 The User Security Subsystem shall generate a Certificate Revocation List (CRL) containing a list of revoked certificates as defined in IEEE Standard 1609.2.

3.2.8.1.2.8 The User Security Subsystem shall accept certificate request messages for 1609.2 Anonymous certificates from the System Users.

3.2.8.1.2.9 The User security Subsystem shall accept 1609.2 Certificate Revocation List (CRL) retrieval requests from other Core Systems.

3.2.8.1.2.10 The User Security Subsystem shall accept certificate request messages from Core System components for 1609.2 Identify Certificates.

3.2.8.1.2.11 If the Certificate Request validation is successful, the User Security Subsystem shall respond with a 1609.2 certificate response message including a signed 1609.2 Identity Certificate to the requesting entity.

3.2.8.1.2.12 If the Certificate Request validation fails, the User Security Subsystem shall respond with a 1609.2 certificate response message with a failure status to the requesting entity.

3.2.8.1.2.13 The User security Subsystem shall accept 1609.2 certificate revocation list (CRL) complete retrieval requests from System Users.

3.2.8.1.2.14 The User security Subsystem shall accept 1609.2 certificate revocation list (CRL) delta update retrieval requests from System Users.

3.2.8.1.2.15 The User Permissions Subsystem shall send the complete 1609.2 certificate revocation list (CRL) to System Users.

3.2.8.1.2.16 The User Permissions Subsystem shall send delta updates of current 1609.2 certificate revocation list (CRL) to System Users.

3.2.8.1.2.17 The User Permissions Subsystem shall send the complete 1609.2 certificate revocation list (CRL) to other Core Systems.

3.2.8.1.2.18 The User Permissions Subsystem shall accept the complete 1609.2 certificate revocation list (CRL) from other Core Systems.

3.2.8.1.2.19 The User Permissions Subsystem shall send delta updates of current 1609.2 certificate revocation list (CRL) to other Core Systems.

3.2.8.1.2.20 The User Permissions Subsystem shall accept delta updates of 1609.2 certificate revocation list (CRL) from other Core Systems.

3.2.8.1.3 X.509 Certificate Authority Functions

3.2.8.1.3.1 The User Security Subsystem shall perform X.509 Certificate Authority functions to System Users in conformance with IETF Public Key Infrastructure for X.509 Certificates (PKIX) standards.

3.2.8.1.3.2 The User Security Subsystem shall support issuance of X.509 v3 Identity certificates to System Users.

3.2.8.1.3.3 The User Security Subsystem shall provide secure storage for X.509 CA private keys.

3.2.8.1.3.4 The User Security Subsystem shall provide secure storage for X.509 root and System User certificates.

3.2.8.1.3.5 The User Security Subsystem shall provide secure storage for X.509 Certificate Revocation Lists (CRL).

3.2.8.1.3.6 The User Security Subsystem shall generate X.509 Certificate Revocation List (CRL) containing a list of revoked X.509 Identity certificates.

3.2.8.1.3.7 The User Security Subsystem shall accept certificate request messages from System Users for X.509 identify certificates.

3.2.8.1.3.8 The User security Subsystem shall accept X.509 Certificate Revocation List (CRL) retrieval requests from other Core Systems.

3.2.8.1.3.9 The User Security Subsystem shall accept certificate request messages from Core System components for X.509 Identify Certificates.

3.2.8.1.3.10 If the Certificate Request validation is successful, the User Security Subsystem shall respond with a X.509 certificate response message including a signed X.509 Identity certificate to the requesting entity.

3.2.8.1.3.11 If the Certificate Request validation fails, the User Security Subsystem shall respond with a X.509 certificate response message with a failure status to the requesting entity.

3.2.8.1.3.12 The User security Subsystem shall accept X.509 certificate revocation list (CRL) complete retrieval requests from System Users.

3.2.8.1.3.13 The User security Subsystem shall accept X.509 certificate revocation list (CRL) delta update retrieval requests from System Users.

3.2.8.1.3.14 The User Permissions Subsystem shall send the complete X.509 certificate revocation list (CRL) to System Users.

3.2.8.1.3.15 The User Permissions Subsystem shall send delta updates of current X.509 certificate revocation list (CRL) to System Users.

3.2.8.1.3.16 The User Permissions Subsystem shall send the complete X.509 certificate revocation list (CRL) to other Core Systems.

3.2.8.1.3.17 The User Permissions Subsystem shall accept the complete X.509 certificate revocation list (CRL) from other Core Systems.

3.2.8.1.3.18 The User Permissions Subsystem shall send delta updates of current X.509 certificate revocation list (CRL) to other Core Systems.

3.2.8.1.3.19 The User Permissions Subsystem shall accept delta updates of X.509 certificate revocation list (CRL) from other Core Systems.

3.2.8.1.3.20 The User Security Subsystem shall send a X.509 root certificates retrieval requests to the x.509 Root provider.

3.2.8.1.4 System Operator interface, logging and retrieval

3.2.8.1.4.1 The User Security Subsystem shall provide a Graphical User interface (GUI) to an authorized System Operator for creating the configuration for its supported services.

3.2.8.1.4.2 The User Security Subsystem shall create System User Identity Certificates based on command from the Operator.

3.2.8.1.4.3 The User Security Subsystem shall create System User Identity Certificates based on input from the User Permissions Subsystem.

3.2.8.1.4.4 The User Security Subsystem shall create System User 1609.2 Anonymous Certificates based on command from the Operator.

3.2.8.1.4.5 The User Security Subsystem shall create System User 1609.2 Anonymous Certificates based on input from the User Permissions Subsystem.

3.2.8.1.4.6 The User Security Subsystem shall send System User Identity Certificates to the System User device.

3.2.8.1.4.7 The User Security Subsystem shall send System User 1609.2 Anonymous Certificates to the System User device.

3.2.8.1.4.8 The User Security Subsystem shall record all System User Identity Certificate creation activities in a log.

3.2.8.1.4.9 The User Security Subsystem shall receive requests for Identify Certificates from System Users.

3.2.8.1.4.10 The User Security Subsystem shall receive requests for 1609.2 Anonymous Certificates from System Users.

3.2.8.1.4.11 If the user validation is successful, the User Security Subsystem shall respond with a 1609.2 Anonymous certificate response message including a set of signed 1609.2 Anonymous certificates to the System User.

3.2.8.1.4.12 If the user validation fails, the User Security Subsystem shall respond with a 1609.2 Anonymous certificate response message with a failure status to the System User.

3.2.8.1.4.13 The User Security Subsystem shall accept certificate request messages for 1609.2 Identity certificates from the System Users.

3.2.8.1.4.14 If the user validation is successful, the User Security Subsystem shall respond with a 1609.2 Identity certificate response message including a set of signed 1609.2 Identity certificates to the System User.

3.2.8.1.4.15 if the user validation fails, the User Security Subsystem shall respond with a 1609.2 Identity certificate response message with a failure status to the System User.

3.2.8.1.4.16 The User Security Subsystem shall accept 1609.2 root certificates retrieval requests from System Users.

3.2.8.1.4.17 The User Security Subsystem shall accept the 1609.2 Certificate Revocation List (CRL) complete retrieval requests from System Users.

3.2.8.1.4.18 The User Security Subsystem shall accept the 1609.2 Certificate Revocation List (CRL) delta update retrieval requests from System Users.

3.2.8.1.4.19 The User Permissions Subsystem shall send the complete 1609.2 Certificate Revocation List (CRL) to other Core Systems.

3.2.8.1.4.20 The User Permissions Subsystem shall accept the complete 1609.2 Certificate Revocation List (CRL) from other Core Systems.

3.2.8.1.4.21 The User Permissions Subsystem shall send delta updates of current 1609.2 Certificate Revocation List (CRL) to other Core Systems.

3.2.8.1.4.22 The User Permissions Subsystem shall accept delta updates of 1609.2 Certificate Revocation List (CRL) from other Core Systems.

3.2.8.1.4.23 The User Security Subsystem shall record all discarded message events in a log.

3.2.8.1.4.24 The User Security Subsystem shall provide Certificate Creation logs to an authorized System Operator.

3.2.8.1.4.25 The User Security Subsystem shall provide discarded message logs to an authorized System Operator.

3.2.8.1.5 Obtaining time

3.2.8.1.5.1 The User Security Subsystem shall accept the time of day from the Time Subsystem.

3.2.8.2 Performance Requirements

3.2.8.2.1 The User Security Subsystem shall process up to [TBD] 1609.2 Certificate Requests per second from System Users.

3.2.8.2.2 The User Security Subsystem shall process up to [TBD] X.509 Certificate Requests per minute from System Users.

3.2.8.2.3 The User Security Subsystem shall generate 1609.2 Certificate Revocation Lists (CRL) periodically at [TBD] rate.

3.2.8.2.4 The User Security Subsystem shall generate X.509 Certificate Revocation Lists (CRL) periodically at [TBD] rate.

3.2.8.3 Interface Requirements

3.2.8.3.1 User Security External Interfaces

3.2.8.3.1.1 The User Security Subsystem shall support an interface for 1609.2 Certificate Authority functions for System Users.

3.2.8.3.1.2 The User Security Subsystem shall support an interface for X.509 Certificate Authority functions for System Users.

3.2.8.3.1.3 The User Security Subsystem shall support IETF PKI X.509 (PKIX) standard interfaces to other X.509 Certificate Authorities.

3.2.8.3.2 User Security Internal Interfaces

3.2.8.3.2.1 The User Security Subsystem shall interface with the Core2Core Subsystem to manage trust credentials.

3.2.8.3.2.2 The User Security Subsystem shall interface with the Data Distribution Subsystem to manage trust credentials.

3.2.8.3.2.3 The User Security Subsystem shall interface with the Misbehavior Management Subsystem to manage trust credentials.

3.2.8.3.2.4 The User Security Subsystem shall interface with the Network Services Subsystem to manage trust credentials.

3.2.8.3.2.5 The User Security Subsystem shall interface with the Service Monitor Subsystem to manage trust credentials.

3.2.8.3.2.6 The User Security Subsystem shall interface with the User Permissions Subsystem to manage trust credentials.

3.2.8.4 Data Requirements

3.2.8.4.1 The User Security Subsystem shall provide secure storage for [TBD] 1609.2 Anonymous Certificates.

3.2.8.4.2 The User Security Subsystem shall provide secure storage for [TBD] 1609.2 Identity Certificates.

3.2.8.4.3 The User Security Subsystem shall provide secure storage for [TBD] X.509 Certificates.

3.2.8.4.4 The User Security Subsystem shall provide secure storage for [TBD] 1609.2 Certificate Revocation Lists (CRL).

3.2.8.4.5 The User Security Subsystem shall provide secure storage for [TBD] X.509 Certificate Revocation Lists (CRL).

3.2.8.4.6 The User Security Subsystem shall provide secure storage on Certificate Authority (CA) locations.

4 Verification Methods

This section contains two tables extracted from the Requirements Database. Table 4-1 lists the system requirements and its verification method. Table 4-2 lists the subsystem requirements and their verification methods. For each requirement, one of the following methods of verification will be listed:

- **Demonstration is** a requirement that the system can demonstrate without external test equipment.
- **Test** is a requirement that requires some external piece of test equipment (e.g. logic analyzer, and/or volt meter).
- **Analyze** is a requirement that is met indirectly through a logical conclusion or mathematical analysis of a result. For example, Algorithms for congestion: the designer may need to show that the requirement is met through the analysis of count and occupancy calculations in software or firmware.
- **Inspection** is verification through a visual comparison. For example, quality of welding may be done through a visual comparison against an in-house standard.

Table 4-1. System Requirements Verification Matrix

Requirement ID	Verification Method
3.1.1.1	D
3.1.1.2	D
3.1.1.4	D
3.1.1.5	D
3.1.1.6	D
3.1.1.7	D
3.1.1.8	D
3.1.1.9	D
3.1.1.10	D
3.1.1.11	D
3.1.1.12	D
3.1.1.13	D
3.1.1.14	D
3.1.1.15	D
3.1.1.16	D
3.1.1.17	D
3.1.1.18	D
3.1.1.19	D
3.1.1.20	D
3.1.1.21	D
3.1.1.22	D
3.1.1.23	D

Requirement ID	Verification Method
3.1.1.24	D
3.1.1.25	D
3.1.1.26	D
3.1.1.27	D
3.1.1.28	D
3.1.1.29	D
3.1.1.30	D
3.1.1.31	D
3.1.1.32	D
3.1.1.33	D
3.1.1.34	D
3.1.1.35	D
3.1.1.36	D
3.1.1.37	D
3.1.1.38	D
3.1.1.39	D
3.1.1.40	D
3.1.1.41	D
3.1.1.42	D
3.1.1.43	D
3.1.1.44	D
3.1.1.45	D

Requirement ID	Verification Method
3.1.1.46	D
3.1.2.1	D
3.1.2.2	D
3.1.2.3	D
3.1.2.4	D
3.1.2.5	D
3.1.2.6	D
3.1.2.7	D
3.1.2.8	D
3.1.2.9	D
3.1.2.10	D
3.1.2.11	D
3.1.2.12	D
3.1.2.13	D
3.1.2.14	D
3.1.2.15	D
3.1.2.16	D
3.1.2.17	D
3.1.2.18	D
3.1.2.19	D
3.1.3.1	D
3.1.3.2	D
3.1.3.3	D
3.1.3.4	D
3.1.3.5	D
3.1.3.6	D
3.1.3.7	D
3.1.3.8	D
3.1.3.9	D
3.1.3.10	D
3.1.3.11	D
3.1.4.1	D
3.1.4.2	D
3.1.4.3	D
3.1.4.4	D
3.1.4.5	D
3.1.4.6	D
3.1.4.7	D
3.1.4.8	D
3.1.4.9	D

Requirement ID	Verification Method
3.1.4.10	D
3.1.5.1.2	D
3.1.5.1.3	D
3.1.5.1.4	D
3.1.5.2.1	D
3.1.5.2.2	A
3.1.5.2.3	A
3.1.5.2.4	D
3.1.5.2.5	D
3.1.5.2.6	I
3.1.5.3.2	T
3.1.5.3.3	D

Table 4-2. Subsystem Requirements Verification Matrix

Requirement ID	Verification Method
3.2.1.1.1	D
3.2.1.1.2	D
3.2.1.1.3	D
3.2.1.1.4	D
3.2.1.1.5	D
3.2.1.1.6	D
3.2.1.1.7	D
3.2.1.1.8	D
3.2.1.1.9	D
3.2.1.1.10	D
3.2.1.1.11	D
3.2.1.1.12	D
3.2.1.1.13	D
3.2.1.1.14	D
3.2.1.1.15	D
3.2.1.1.16	D
3.2.1.1.17	D
3.2.1.1.18	D
3.2.1.1.19	D
3.2.1.1.20	D
3.2.1.1.21	D
3.2.1.1.22	D
3.2.1.1.23	D
3.2.1.1.24	D
3.2.1.1.25	D
3.2.1.1.25.1	D
3.2.1.1.26	D
3.2.1.1.26.1	D
3.2.1.1.26.2	D
3.2.1.1.26.3	D
3.2.1.1.26.4	D
3.2.1.1.27	D
3.2.1.1.27.1	D
3.2.1.1.27.2	D
3.2.1.1.27.3	D
3.2.1.1.27.4	D
3.2.1.1.27.5	D
3.2.1.1.27.6	D
3.2.1.1.27.7	D

Requirement ID	Verification Method
3.2.1.1.27.8	D
3.2.1.1.28	D
3.2.1.1.28.1	D
3.2.1.1.28.2	D
3.2.1.1.28.3	D
3.2.1.1.28.4	D
3.2.1.1.29	D
3.2.1.1.29.1	D
3.2.1.1.29.2	D
3.2.1.1.30	D
3.2.1.1.31	D
3.2.1.1.32	D
3.2.1.1.33	D
3.2.1.2.1	T
3.2.1.2.2	T
3.2.1.3.1	D
3.2.1.3.2	D
3.2.1.3.3	D
3.2.1.3.4	D
3.2.1.3.5	D
3.2.1.4.1	D
3.2.1.4.2	D
3.2.1.4.3	D
3.2.1.4.4	D
3.2.2.1.1.1	D
3.2.2.1.1.2	D
3.2.2.1.1.3	D
3.2.2.1.1.4	D
3.2.2.1.1.5	D
3.2.2.1.1.6	D
3.2.2.1.1.7	D
3.2.2.1.1.8	D
3.2.2.1.2	D
3.2.2.1.3	D
3.2.2.1.3.1	D
3.2.2.1.3.2	D
3.2.2.1.4	D
3.2.2.1.5	D
3.2.2.1.6	D

Requirement ID	Verification Method
3.2.2.1.7	D
3.2.2.1.8.1	D
3.2.2.1.9.1	D
3.2.2.1.10	D
3.2.2.1.10.1	D
3.2.2.1.10.2	D
3.2.2.1.10.3	D
3.2.2.1.10.4	D
3.2.2.1.10.5	D
3.2.2.1.10.6	D
3.2.2.1.10.7	D
3.2.2.1.10.8	D
3.2.2.1.10.9	D
3.2.2.1.10.10	D
3.2.2.1.11	D
3.2.2.1.12	D
3.2.2.1.13	D
3.2.2.1.13.1	D
3.2.2.1.14	D
3.2.2.1.15	D
3.2.2.1.16	D
3.2.2.1.17	D
3.2.2.1.18	D
3.2.2.1.19	D
3.2.2.1.20.1	D
3.2.2.1.20.2	D
3.2.2.1.20.3	D
3.2.2.1.20.4	D
3.2.2.1.20.5	D
3.2.2.1.20.6	D
3.2.2.1.20.7	D
3.2.2.1.20.8	D
3.2.2.1.20.9	D
3.2.2.1.20.10	D
3.2.2.1.20.11.1	D
3.2.2.1.21.1	D
3.2.2.1.21.2	D
3.2.2.1.21.3	D
3.2.2.1.21.4	D
3.2.2.1.21.5	D

Requirement ID	Verification Method
3.2.2.1.21.6	D
3.2.2.1.21.7	D
3.2.2.1.21.8	D
3.2.2.1.22.1	D
3.2.2.2.1	T
3.2.2.3.1	D
3.2.2.3.2	D
3.2.2.3.3	D
3.2.2.4.1	D
3.2.2.4.2	D
3.2.2.4.3	D
3.2.2.4.4	D
3.2.2.4.5	D
3.2.2.4.6	D
3.2.2.4.7	D
3.2.3.1.1	T
3.2.3.1.2.1	D
3.2.3.1.2.3	D
3.2.3.1.2.4	D
3.2.3.1.3.1	D
3.2.3.1.3.2	D
3.2.3.1.3.3	D
3.2.3.1.3.4	D
3.2.3.1.3.5	D
3.2.3.1.3.6	D
3.2.3.1.3.7	D
3.2.3.1.3.8	D
3.2.3.1.4.1	D
3.2.3.1.4.2	D
3.2.3.1.4.3	D
3.2.3.1.4.4	D
3.2.3.1.4.5	D
3.2.3.1.4.6	D
3.2.3.1.4.7	D
3.2.3.1.5.1	D
3.2.3.1.5.2	D
3.2.3.1.5.2.1	D
3.2.3.1.5.2.2	D
3.2.3.1.5.3	D
3.2.3.1.5.4	D

Requirement ID	Verification Method
3.2.3.1.5.5	D
3.2.3.1.6.1	D
3.2.3.2.1	T
3.2.3.2.2	T
3.2.3.2.3	T
3.2.3.3.1	D
3.2.3.3.2	D
3.2.3.3.3	D
3.2.3.4.1	D
3.2.3.4.2	D
3.2.3.4.3	D
3.2.3.4.4	D
3.2.3.4.5	D
3.2.3.4.6	D
3.2.4.1.1.1	I
3.2.4.1.1.2	D
3.2.4.1.1.3	D
3.2.4.1.1.4	D
3.2.4.1.1.5	D
3.2.4.1.1.6	D
3.2.4.1.1.7	D
3.2.4.1.1.8	D
3.2.4.1.1.9	D
3.2.4.1.2.1	D
3.2.4.1.2.2	D
3.2.4.1.2.3	D
3.2.4.1.3.1	D
3.2.4.1.3.2	D
3.2.4.1.3.3	D
3.2.4.1.3.4	D
3.2.4.1.3.5	D
3.2.4.1.3.6	D
3.2.4.1.3.7	D
3.2.4.1.3.8	D
3.2.4.1.3.9	D
3.2.4.1.3.10	D
3.2.4.1.3.11	D
3.2.4.1.3.12	D
3.2.4.1.3.13	D
3.2.4.1.3.14	D

Requirement ID	Verification Method
3.2.4.1.4.1	D
3.2.4.2.1	T
3.2.4.2.2	T
3.2.4.3.1	D
3.2.4.3.2	D
3.2.4.3.3	D
3.2.4.3.4	D
3.2.4.4.1	D
3.2.5.1.1	D
3.2.5.1.1.1	D
3.2.5.1.1.2	D
3.2.5.1.1.3	D
3.2.5.1.1.4	D
3.2.5.1.1.5	D
3.2.5.1.1.6	D
3.2.5.1.1.7	D
3.2.5.1.1.8	D
3.2.5.1.1.9	D
3.2.5.1.1.10	D
3.2.5.1.1.11	D
3.2.5.1.1.12	D
3.2.5.1.1.13	D
3.2.5.1.1.14	D
3.2.5.1.1.15	D
3.2.5.1.1.16	D
3.2.5.1.1.17	D
3.2.5.1.1.18	D
3.2.5.1.2	D
3.2.5.1.3	D
3.2.5.1.4	D
3.2.5.1.5	D
3.2.5.1.6	D
3.2.5.1.7	D
3.2.5.1.8	D
3.2.5.1.8.1	D
3.2.5.1.9	D
3.2.5.1.10	D
3.2.5.1.11	D
3.2.5.1.11.1	D
3.2.5.1.11.2	D

Requirement ID	Verification Method
3.2.5.1.11.3	D
3.2.5.1.11.4	D
3.2.5.1.11.5	D
3.2.5.1.11.6	D
3.2.5.1.11.7	D
3.2.5.1.11.8	D
3.2.5.1.11.9	D
3.2.5.1.11.10	D
3.2.5.1.11.11	D
3.2.5.1.11.12	D
3.2.5.1.12	D
3.2.5.1.12.1	D
3.2.5.1.12.2	D
3.2.5.1.12.3	D
3.2.5.1.12.4	D
3.2.5.1.12.5	D
3.2.5.1.13	D
3.2.5.1.14	D
3.2.5.1.15	D
3.2.5.1.16	D
3.2.5.1.17	D
3.2.5.1.18	D
3.2.5.1.19	D
3.2.5.1.20	D
3.2.5.1.21	D
3.2.5.1.22	D
3.2.5.2.1	T
3.2.5.2.2	T
3.2.5.2.3	T
3.2.5.2.4	T
3.2.5.2.5	D
3.2.5.3.1	D
3.2.5.3.2	D
3.2.5.3.3	D
3.2.5.4.2	D
3.2.5.4.3	D
3.2.5.4.4	D
3.2.5.4.5	D
3.2.5.4.6	D
3.2.6.1.1	D

Requirement ID	Verification Method
3.2.6.1.2	D
3.2.6.1.3	D
3.2.6.1.4	D
3.2.6.1.5	D
3.2.6.1.6	D
3.2.6.1.7	D
3.2.6.1.8	D
3.2.6.1.9	D
3.2.6.1.10	D
3.2.6.1.11	D
3.2.6.1.12	D
3.2.6.2.1	T
3.2.6.2.2	T
3.2.6.3.1	D
3.2.6.3.2	D
3.2.7.1.1.1	T
3.2.7.1.1.2	T
3.2.7.1.1.3	T
3.2.7.1.1.4	T
3.2.7.1.2.1	T
3.2.7.1.2.2	T
3.2.7.1.2.3	T
3.2.7.1.2.4	T
3.2.7.1.2.5	T
3.2.7.1.2.6	T
3.2.7.1.2.7	T
3.2.7.1.2.8	T
3.2.7.1.2.9	T
3.2.7.1.2.10	T
3.2.7.1.2.11	T
3.2.7.1.2.12	T
3.2.7.1.2.13	T
3.2.7.1.2.14	T
3.2.7.1.3.1	D
3.2.7.2.1	T
3.2.7.2.2	T
3.2.7.2.3	T
3.2.7.2.4	T
3.2.7.3.1	D
3.2.7.3.1.1	D

Requirement ID	Verification Method
3.2.7.3.1.2	D
3.2.7.3.1.3	D
3.2.7.3.1.4	D
3.2.7.3.2	D
3.2.7.3.2.1	D
3.2.7.3.2.2	D
3.2.7.3.2.3	D
3.2.7.3.2.4	D
3.2.7.3.2.5	D
3.2.7.3.2.6	D
3.2.7.3.2.7	D
3.2.7.3.2.8	D
3.2.7.3.3	D
3.2.7.3.3.1	D
3.2.7.3.3.2	D
3.2.7.3.3.3	D
3.2.7.3.3.4	D
3.2.7.3.3.5	D
3.2.7.3.3.6	D
3.2.7.3.3.7	D
3.2.7.3.3.8	D
3.2.7.3.3.9	D
3.2.7.3.4	D
3.2.7.3.4.1	D
3.2.7.3.4.2	D
3.2.7.3.4.3	D
3.2.7.3.4.4	D
3.2.7.4.1	D
3.2.7.4.2	D
3.2.7.4.3	D
3.2.7.4.4	D
3.2.7.4.5	D
3.2.7.4.6	D
3.2.7.4.7	D
3.2.8.1.1.1	T
3.2.8.1.1.2	T
3.2.8.1.1.3	T
3.2.8.1.1.4	T
3.2.8.1.1.5	T
3.2.8.1.1.6	T

Requirement ID	Verification Method
3.2.8.1.1.7	T
3.2.8.1.1.8	T
3.2.8.1.1.9	T
3.2.8.1.1.10	T
3.2.8.1.1.11	T
3.2.8.1.1.12	T
3.2.8.1.1.13	T
3.2.8.1.1.14	T
3.2.8.1.1.15	T
3.2.8.1.2.1	T
3.2.8.1.2.2	T
3.2.8.1.2.3	T
3.2.8.1.2.4	T
3.2.8.1.2.5	T
3.2.8.1.2.6	T
3.2.8.1.2.7	T
3.2.8.1.2.8	T
3.2.8.1.2.9	T
3.2.8.1.2.10	T
3.2.8.1.2.11	T
3.2.8.1.2.12	T
3.2.8.1.2.13	T
3.2.8.1.2.14	T
3.2.8.1.2.15	T
3.2.8.1.2.16	T
3.2.8.1.2.17	T
3.2.8.1.2.18	T
3.2.8.1.2.19	T
3.2.8.1.2.20	T
3.2.8.1.3.1	T
3.2.8.1.3.2	T
3.2.8.1.3.3	T
3.2.8.1.3.4	T
3.2.8.1.3.5	T
3.2.8.1.3.6	T
3.2.8.1.3.7	T
3.2.8.1.3.8	T
3.2.8.1.3.9	T
3.2.8.1.3.10	T
3.2.8.1.3.11	T

Requirement ID	Verification Method
3.2.8.1.3.12	T
3.2.8.1.3.13	T
3.2.8.1.3.14	T
3.2.8.1.3.15	T
3.2.8.1.3.16	T
3.2.8.1.3.17	T
3.2.8.1.3.18	T
3.2.8.1.3.19	T
3.2.8.1.3.20	T
3.2.8.1.4.1	T
3.2.8.1.4.2	T
3.2.8.1.4.3	T
3.2.8.1.4.4	T
3.2.8.1.4.5	T
3.2.8.1.4.6	T
3.2.8.1.4.7	T
3.2.8.1.4.8	D
3.2.8.1.4.9	D
3.2.8.1.4.10	D
3.2.8.1.4.11	D
3.2.8.1.4.12	D
3.2.8.1.4.13	D
3.2.8.1.4.14	D
3.2.8.1.4.15	D
3.2.8.1.4.16	D
3.2.8.1.4.17	D
3.2.8.1.4.18	D
3.2.8.1.4.19	D
3.2.8.1.4.20	D
3.2.8.1.4.21	D
3.2.8.1.4.22	D
3.2.8.1.4.23	D
3.2.8.1.4.24	D
3.2.8.1.4.25	D
3.2.8.1.5.1	D
3.2.8.2.1	T
3.2.8.2.2	T
3.2.8.2.3	T
3.2.8.2.4	T
3.2.8.3.1.1	T

Requirement ID	Verification Method
3.2.8.3.2.1	T
3.2.8.3.2.2	T
3.2.8.4.1	D
3.2.8.4.2	D
3.2.8.4.3	D
3.2.8.4.4	D
3.2.8.4.5	D
3.2.8.4.6	D

5 Supporting Documentation

This section provides references or other information that may add to the understanding of the Requirements without going elsewhere. This section contains the Core System Needs, Internet Based Communication Standards, and Action Verb definitions.

5.1 Core System Needs

The following table contains a copy of the Core System Needs from the Core System Concept of Operations document. These Core System Needs are the basis for the requirements in this document. Section 6 on page 75 includes the traceability from these needs to the requirements and vice versa.

ID	Core System Need	Rationale	Priority	Subsystem
1	Data Protection	The Core System needs to protect data it handles from unauthorized access. This is required to support applications that exchange sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.	Essential	User Security
2	Core Trust	The Core System needs to establish trust with its System Users. Such trust relationships are necessary so that the Core System can be assured that System Users are who they say they are, and therefore trust the source.	Essential	User Security
3	System User Trust	The Core System needs to facilitate trust between System Users. Such trust relationships are necessary so that system users can be assured that other system users "are who they say they are," and therefore trust the source and data they receive from other system users.	Essential	User Security

ID	Core System Need	Rationale	Priority	Subsystem
4	Core Trust Revocation	The Core System needs to revoke the trust relationship it has with its System Users when necessary. A trusted system user may operate in a fashion that indicates it should no longer be trusted, in which case the Core System must have a way of revoking that trust.	Essential	Misbehavior Management, User Security
5	System User Trust Revocation	The Core System needs to facilitate the revocation of the trust relationships between System Users when necessary. A trusted System User may operate in a fashion that indicates it should no longer be trusted, in which case the Core System must have a way of facilitating revocation of trust between System Users.	Essential	Misbehavior Management, User Security
6	Authorization Management	The Core System needs to manage authorization mechanisms to define roles, responsibilities and permissions for System Users. This enables the Core System to establish operational environments where different System Users may have different capabilities in terms of accessing Core services and interacting with one another. For instance, some Mobile elements may be authorized to request signal priority, or some Centers may be permitted to use the geographic broadcast service, while those without those permissions would not.	Essential	User Permission

ID	Core System Need	Rationale	Priority	Subsystem
7	Authorization Verification	The Core System needs to verify that System Users and Core Operations Personnel are authorized to perform an attempted operation. This enables the Core System to restrict operations to those users are permitted to use those operations. For example, geo-broadcast may be restricted to transportation or public safety agencies, so other users may be prohibited from performing geo-broadcast.	Essential	User Permission
8	Misbehavior Identification	The Core System needs to identify System Users acting as bad actors. Bad actors are not necessarily malicious; they could be malfunctioning devices that may interfere with other System Users, Communications Layer systems or the Core System. Identifying bad actors enables subsequent action to protect the integrity of all users sharing the transportation environment.	Desirable	Misbehavior Management
9	Time Base	The Core System needs to operate on a common time base. Coordination of time between the internal systems that operate the Core System prevents internal synchronization errors and enables time-sensitive interactions with System Users.	Essential	Time

ID	Core System Need	Rationale	Priority	Subsystem
10	Data Request	The Core System needs to provide a mechanism for data consumers to request data that is produced by data providers. This is a single request for a subscription to a certain type of data, and subsequent modification of the request to change data types or subscription parameters. Parameters include data frequency, type and location of where the data was generated. This enables the distribution of anonymously-provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example this includes data type, geographic range, frequency and sampling rate. This request method supports a wide variety of user needs, from planners requesting all traffic data all the time, to traveler information services requesting a subset of traffic data, to weather information services only interested in windshield wiper status for vehicles in a specific area.	Desirable	Data Distribution

ID	Core System Need	Rationale	Priority	Subsystem
11	Data Provision	The Core System needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics need to include type, frequency and location where data was generated, so that users that have requested data (see need data request) can differentiate between available data. This need enables data providers to direct the data they create to data consumers, and serves as the provider-side corollary to the data request need. This supports a variety of applications, including those focused on the center provision of data to users. It also serves as the answer to the System User's question of "I have data, how do I provide it and to whom?"	Desirable	Data Distribution

ID	Core System Need	Rationale	Priority	Subsystem
12	Data Forward	The Core System needs to provide a mechanism to distribute data that is produced by a system user acting as a data provider and requested by another system user. The Core System needs to provide this distribution mechanism, rather than relying on individual provider-consumer relationships, because multiple consumers may want access to the same data. By having the Core System distribute the data, system users are relieved of the need to transmit the data multiple times. Also, some data that may be critical to the proper functioning of mandatory applications, such as data supporting geo-location of users (position corrections), time base data and roadway geometry data, all of which likely comes from a single source and needs to be distributed to large numbers of system users. Additionally, system users may interact over resource-constrained communication links, so Core-provided data redistribution reduces the potential load on those links.	Desirable	Data Distribution
13	Network Connectivity	The Core System needs to connect to the Internet. This allows the Core to provide services to any System User capable of connecting to the Internet.	Desirable	Network Services

ID	Core System Need	Rationale	Priority	Subsystem
14	Geographic Broadcast	The Core System needs to provide the information necessary for System Users who wish to communicate with a group of System Users in a specific area to do so. This capability enables System Users to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of applications that might use this include Amber Alerts, traffic information, and air quality alerts.	Desirable	Data Distribution, Network Services
15	Core System Service Status	The Core System needs to be able to accept and maintain the status of core system services and provide accurate status information to System Users. System Users may not be able to access a Core System service (because of their location for example) and would want to know where and when they could expect access to the Service.	Desirable	Service Monitor
16	System Integrity Protection	The Core System needs to protect the integrity of the Core System. This includes defense against the loss of integrity from a deliberate attack, software bug, environmental or hardware failure, as well as mitigation strategies to facilitate a predictable return to normal operations. Protection and controlled restoration of normal operations ensures that System Users have a high confidence in the security of the information they entrust to the Core System.	Essential	Service Monitor

ID	Core System Need	Rationale	Priority	Subsystem
17	System Availability	The Core System needs to be available for System Users to access Core System Services. This ensures that System Users have a high confidence in the performance of the Core System, and can rely on its services to accomplish their objectives.	Essential	Service Monitor
18	System Operational Performance Monitoring	The Core System needs to monitor its performance. This includes the status of interfaces, services, and metrics for the number of requests and the resolution of those requests. Monitoring the performance of Core System services and interfaces is necessary to understand when the system is operating properly, and to gauge when the system may be nearing capacity so that action may be taken to prevent the system from failing to provide services, e.g. maximum number of transactions/second, or internal communication bandwidth.	Essential	Service Monitor
19	Core System Independence	The Core System needs to be able to be independently deployed and operated providing Core System services to all System Users within its jurisdictional scope. This ensures that one entity's Core System deployment is not contingent on or dependent on another for basic functionality.	Essential	Core2Core, Service Monitor, User Permission, User Security

ID	Core System Need	Rationale	Priority	Subsystem
20	Core System Interoperability	The Core System needs to provide services in such a way that if a mobile user moves into an area of another Core System their interface to the Core System still operates. This helps manage user expectations and helps ensure that when a mobile user subscribes to a service or installs an application the user experience is consistent across multiple Core Systems.	Essential	Core2Core, Data Distribution, Misbehavior Management, Network Services, Service Monitor, Time, User Security
21	Core System Interdependence	The Core System needs to operate in coordination with other Core Systems. This ensures that Core services deliver information that is consistent with information delivered by other Core systems, which will help avoid inconsistencies and incompatibilities between Cores and between Mobile users interacting with multiple Cores.	Essential	Core2Core, Data Distribution, Misbehavior Management, Network Services, Time, User Security
22	Core System Data Protection	The Core System needs to protect data it maintains from unauthorized access. This ensures that information held by the Core, which may include sensitive information about System Users, is accessed only by authorized users.	Essential	Service Monitor, User Security

ID	Core System Need	Rationale	Priority	Subsystem
23	Anonymity Preservation	The Core System needs to preserve the anonymity of anonymous System Users that use its services. This ensures that System Users communicating with the Core who wish to remain anonymous will not have their anonymity breached as a result of communicating with the Core.	Essential	User Security

5.2 State and Modes

The states and modes of operation of the Core System are described in this section. The following list identifies the states that will be considered[3,4]:

- Installation (Core-wide only)
- Operational
- Maintenance
- Training (Core-wide only)
- Standby

Two or more of these states may occur simultaneously within the same Core as different subsystems may be in different states. Subsystems may be in any combination of Operational, Maintenance, and Standby states. Training and Installation states are Core-wide; if the Core is in one of these two states, all subsystems are in that state.

The major states are described in more detail below:

- Installation: This state includes all pre-operational activities necessary to plan, develop, install and verify the procedures and system configurations used to support the Core System. The Installation state for the Core System includes the following activities:
  - Planning and preparation
  - Coordinating with participating external agencies
  - Detailed planning of resources
  - Resource acquisition
  - Installation

[3] Other states may be defined as needed in later documents.

[4] Depending on local policies and procedures, a particular Core System may deviate from these states. For example, a training state may not be supported at all.

  - Preparation and verification of subsystem configurations and timelines (different configurations may be applicable based on time of day, day of week etc.)
  - System checkout (the activities necessary to ensure that the configuration of Core subsystems and interfaces are per the planning documentation and verified ready to support operations)
  - Operating the Core System in parallel with current systems. Depending on the locality, the Installation state could take a few weeks/months. For a new locality, it could take a few months/years in duration.
  - System check-out
- Operational: This state includes all activities during the normal conduct of operations. This state also needs to be able to handle support for services from other Cores including fail-over and/or degraded services. The Operational state includes the following activities:
  - Loading, verifying and granting security certificates to System Users
  - Providing timing services
  - Facilitating real-time and near real-time data exchanges
  - Providing network services
  - Enabling application processing
  - Monitoring health of Core System
  - Managing Core System resources
  - Accommodating service support for other degraded or non-operational Cores
- Maintenance: An administrator places the Core or a particular subsystem in a Maintenance state to replace an impaired component or to upgrade a component(s) of the Core. Depending on the nature of maintenance planned, the impact on the Core System's ability to provide services may be impacted. Also, its ability to manage itself and provide visibility into how it is performing may be impacted.
- Training: The Core System will be placed in a Training state when it is used for imparting training on the Core features. Certain features like real-time display of log messages and debug messages may be enabled in the Training state which may not otherwise be accessible under normal conditions.
- Standby: The Core System or subsystem operating in a Standby state will be providing backup to one or more other Cores or other Core subsystems. From the standby state the Core or subsystem may take over the functions of another Core or subsystem if required. When operating in Standby state, the Core or subsystem should be continually evaluated on its ability to switch-in and take provide services for the Core or subsystem it is supporting.

Figure 5-1 captures the states of the Core System and the transitions possible from one state to another.

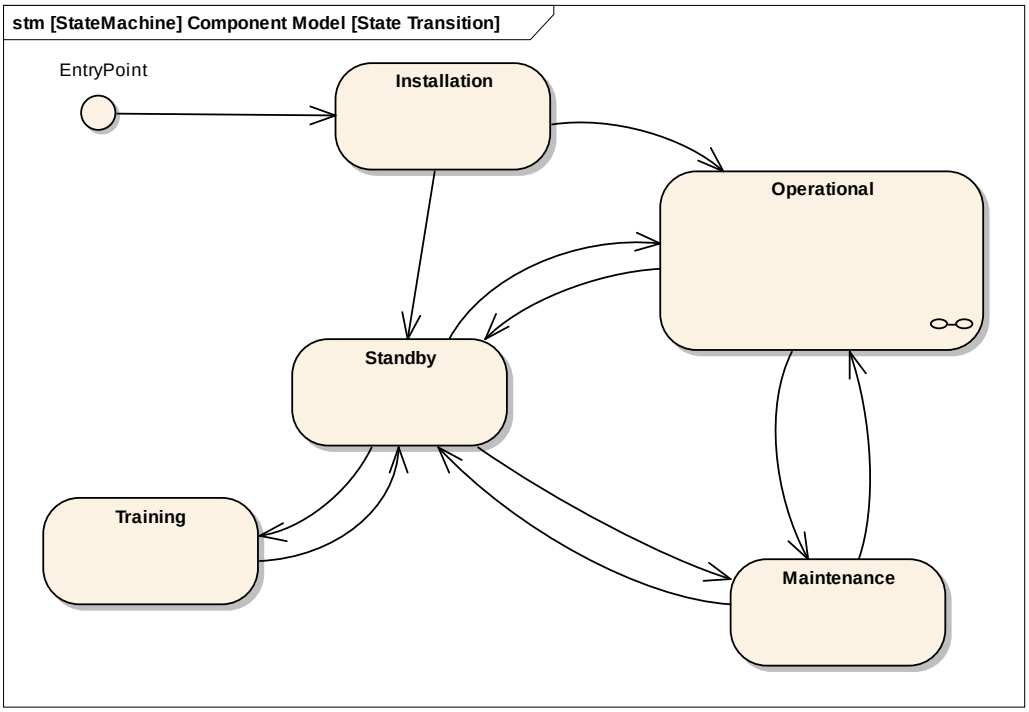


Figure 5-1. Core State Transition Diagram

While in the Operational state, each subsystem may be in one of the following modes:

- Normal mode: In the normal mode, there is little or no functional or performance impacts on the ability of the subsystem to provide its services. In addition, the Service Monitor provides good visibility into how the subsystem is performing.
- Degraded mode: In the degraded mode, the subsystem is impaired to a significant extent: its ability to provide services is greatly reduced or eliminated completely. Also, Service Monitor's ability to manage the subsystem may be impaired.
- Restricted mode: In the restricted mode, the subsystem is capable of performing as expected; however certain services or features are disabled to support a specific event such as an evacuation. The restriction is determined by operators/entities outside of the system and subsequently implemented by the system in response to an authorized operation (command) from the external entity. This may also be implemented via a policy-based management system whereby policies (as specified by an authorized external entity) are automatically implemented by the Core System in response to detection of events, behaviors or performance thresholds. In a restricted mode, the Core System could curtail the use of particular subsystems to privileged users, such first responders and other emergency personnel.
- Degraded/Restricted Mode: If during the course of operating in a restricted mode there is a loss of functionality, or if while in degraded mode there is a need to enter restricted mode, the subsystem may enter the degraded/restricted mode. This mode is a combination of the restricted and degraded modes, where subsystem services are offered only to particular users, but performance is degraded.

Figure 5-2 illustrates subsystem modes as part of the Operational State.

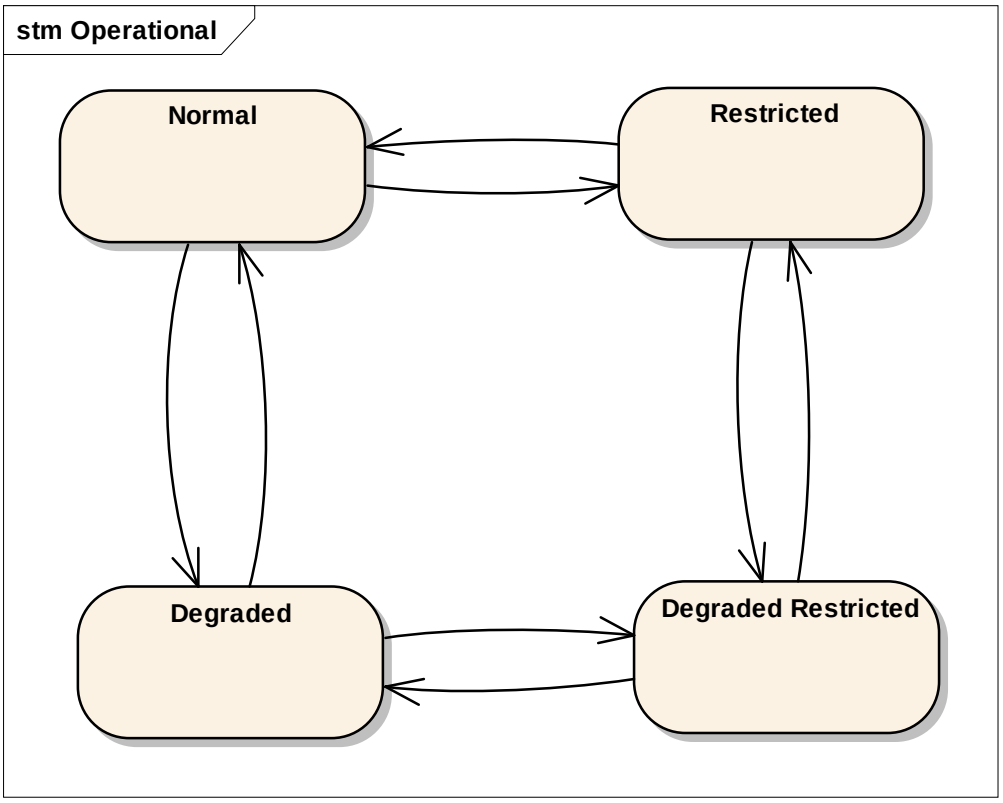


Figure 5-2. Subsystem Operational Modes Diagram

5.3 Internet Based Communications Standards

The section contains a listing of Internet Engineering Task Force (IETF) Request for Comments (RFCs). These standards define how internet communications systems are implemented. The Core System implementations will need to be aware of the developments in this industry to ensure interoperable communications with external systems.

These tables provide the document number, title, date of the current publication, its development status and an indication of whether filing disclosures about Intellectual Property Rights (IPR).

Table 5-1. Network Time Protocol (NTP) Standards

Document	Title	Date	Status
RFC 5905 (draft-ietf-ntp-ntpv4-proto)	Network Time Protocol Version 4: Protocol and Algorithms Specification	2010-06	RFC 5905 (Proposed Standard) Errata
RFC 5906 (draft-ietf-ntp-autokey)	Network Time Protocol Version 4: Autokey Specification	2010-06	RFC 5906 (Informational)
RFC 5907 (draft-ietf-ntp-ntpv4-mib)	Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)	2010-06	RFC 5907 (Proposed Standard) Errata

Document	Title	Date	Status
RFC 5908 (draft-ietf-ntp-dhcpv6-ntp-opt)	Network Time Protocol (NTP) Server Option for DHCPv6	2010-06	RFC 5908 (Proposed Standard)

Source: http://datatracker.ietf.org/wg/ntp/

Table 5-2. PKI X.509 Standards

Document	Title	Date	Status	Ipr
Active Internet-Drafts				
draft-ietf-pkix-certimage-11	Internet X.509 Public Key Infrastructure - Certificate Image	2011-02-15	RFC Ed Queue (for 55 days) RFC Editor State: RFC-EDITOR	
draft-ietf-pkix-eai-addresses-00	Internationalized Email Addresses in X.509 certificates	2011-03-07	I-D Exists	
draft-ietf-pkix-ocspagility-10	Online Certificate Status Protocol Algorithm Agility	2011-03-11	RFC Ed Queue (for 27 days) RFC Editor State: EDIT	
draft-ietf-pkix-pubkey-caps-02	S/MIME Capabilities for Public Key Definitions	2011-04-06 new	I-D Exists	
draft-ietf-pkix-rfc2560bis-03	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	2011-04-05 new	I-D Exists	
draft-ietf-pkix-rfc5272-bis-03	Certificate Management over CMS (CMC) Updates	2011-04-06 new	I-D Exists	
draft-ietf-pkix-rfc5280-clarifications-02	Clarifications to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2011-03-28	I-D Exists	
RFC 2459 (draft-ietf-pkix-ipki-part1)	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	1999-01	RFC 2459 (Proposed Standard) Obsoleted by RFC 3280 Errata	
RFC 2510 (draft-ietf-pkix-ipki3cmp)	Internet X.509 Public Key Infrastructure Certificate Management Protocols	1999-03	RFC 2510 (Proposed Standard) Obsoleted by RFC 4210	
RFC 2511 (draft-ietf-pkix-crmf)	Internet X.509 Certificate Request Message Format	1999-03	RFC 2511 (Proposed Standard) Obsoleted by RFC 4211	
RFC 2527 (draft-ietf-pkix-ipki-part4)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	1999-03	RFC 2527 (Informational) Obsoleted by RFC 3647 Errata	
RFC 2528 (draft-ietf-pkix-ipki-kea)	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	1999-03	RFC 2528 (Informational)	
RFC 2559 (draft-ietf-pkix-ipki2opp)	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	1999-04	RFC 2559 (Historic) Obsoleted by RFC 3494	
RFC 2560 (draft-ietf-pkix-ocsp)	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	1999-06	RFC 2560 (Proposed Standard) Errata	

Document	Title	Date	Status	Ipr
RFC 2585 (draft-ietf-pkix-opp-ftp-http)	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	1999-05	RFC 2585 (Proposed Standard) Errata	
RFC 2587 (draft-ietf-pkix-ldapv2-schema)	Internet X.509 Public Key Infrastructure LDAPv2 Schema	1999-06	RFC 2587 (Proposed Standard) Obsoleted by RFC 4523	
RFC 2797 (draft-ietf-pkix-cmc)	Certificate Management Messages over CMS	2000-04	RFC 2797 (Proposed Standard) Obsoleted by RFC 5272	
RFC 2875 (draft-ietf-pkix-dhpop)	Diffie-Hellman Proof-of-Possession Algorithms	2000-07	RFC 2875 (Proposed Standard)	
RFC 3029 (draft-ietf-pkix-dcs)	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	2001-02	RFC 3029 (Experimental)	
RFC 3039 (draft-ietf-pkix-qc)	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	2001-01	RFC 3039 (Proposed Standard) Obsoleted by RFC 3739	
RFC 3161 (draft-ietf-pkix-time-stamp)	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	2001-08	RFC 3161 (Proposed Standard) Updated by RFC 5816 Errata	
RFC 3279 (draft-ietf-pkix-ipki-pkalgs)	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002-04	RFC 3279 (Proposed Standard) Updated by RFC 4055, RFC 4491, RFC 5480, RFC 5758 Errata	
RFC 3280 (draft-ietf-pkix-new-part1)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002-04	RFC 3280 (Proposed Standard) Obsoleted by RFC 5280 Updated by RFC 4325, RFC 4630 Errata	1
RFC 3281 (draft-ietf-pkix-ac509prof)	An Internet Attribute Certificate Profile for Authorization	2002-04	RFC 3281 (Proposed Standard) Obsoleted by RFC 5755 Errata	
RFC 3379 (draft-ietf-pkix-dpv-dpd-req)	Delegated Path Validation and Delegated Path Discovery Protocol Requirements	2002-09	RFC 3379 (Informational)	
RFC 3628 (draft-ietf-pkix-pr-tsa)	Policy Requirements for Time-Stamping Authorities (TSAs)	2003-11	RFC 3628 (Informational)	
RFC 3647 (draft-ietf-pkix-ipki-new-rfc2527)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	2003-11	RFC 3647 (Informational) Errata	
RFC 3709 (draft-ietf-pkix-logotypes)	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates	2004-02	RFC 3709 (Proposed Standard) Errata	
RFC 3739 (draft-ietf-pkix-sonof3039)	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	2004-03	RFC 3739 (Proposed Standard)	

Document	Title	Date	Status	Ipr
RFC 3770 (draft-ietf-pkix-wlan-extns)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2004-05	RFC 3770 (Proposed Standard) Obsoleted by RFC 4334 Errata	
RFC 3779 (draft-ietf-pkix-x509-ipaddr-as-extn)	X.509 Extensions for IP Addresses and AS Identifiers	2004-06	RFC 3779 (Proposed Standard) Errata	
RFC 3820 (draft-ietf-pkix-proxy)	Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	2004-06	RFC 3820 (Proposed Standard)	
RFC 3874 (draft-ietf-pkix-sha224)	A 224-bit One-way Hash Function: SHA-224	2004-09	RFC 3874 (Informational)	
RFC 4043 (draft-ietf-pkix-pi)	Internet X.509 Public Key Infrastructure Permanent Identifier	2005-05	RFC 4043 (Proposed Standard) Errata	
RFC 4055 (draft-ietf-pkix-rsa-pkalgs)	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2005-06	RFC 4055 (Proposed Standard) Updated by RFC 5756 Errata	
RFC 4059 (draft-ietf-pkix-warranty-extn)	Internet X.509 Public Key Infrastructure Warranty Certificate Extension	2005-05	RFC 4059 (Informational)	
RFC 4158 (draft-ietf-pkix-certpathbuild)	Internet X.509 Public Key Infrastructure: Certification Path Building	2005-09	RFC 4158 (Informational)	
RFC 4210 (draft-ietf-pkix-rfc2510bis)	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)	2005-09	RFC 4210 (Proposed Standard) Errata	
RFC 4211 (draft-ietf-pkix-rfc2511bis)	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	2005-09	RFC 4211 (Proposed Standard) Errata	
RFC 4325 (draft-ietf-pkix-crlaia)	Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension	2005-12	RFC 4325 (Proposed Standard) Obsoleted by RFC 5280	
RFC 4334 (draft-ietf-pkix-rfc3770bis)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2006-02	RFC 4334 (Proposed Standard) Errata	
RFC 4386 (draft-ietf-pkix-pkixrep)	Internet X.509 Public Key Infrastructure Repository Locator Service	2006-02	RFC 4386 (Experimental)	
RFC 4387 (draft-ietf-pkix-certstore-http)	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP	2006-02	RFC 4387 (Proposed Standard)	
RFC 4476 (draft-ietf-pkix-acpolicies-extn)	Attribute Certificate (AC) Policies Extension	2006-05	RFC 4476 (Proposed Standard)	
RFC 4491 (draft-ietf-pkix-gost-cppk)	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	2006-05	RFC 4491 (Proposed Standard) Errata	

Document	Title	Date	Status	Ipr
RFC 4630 (draft-ietf-pkix-cert-utf8)	Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2006-08	RFC 4630 (Proposed Standard) Obsoleted by RFC 5280	
RFC 4683 (draft-ietf-pkix-sim)	Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)	2006-10	RFC 4683 (Proposed Standard) Errata	
RFC 4985 (draft-ietf-pkix-srvsan)	Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name	2007-08	RFC 4985 (Proposed Standard) Errata	
RFC 5019 (draft-ietf-pkix-lightweight-ocsp-profile)	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments	2007-09	RFC 5019 (Proposed Standard)	
RFC 5055 (draft-ietf-pkix-scvp)	Server-Based Certificate Validation Protocol (SCVP)	2007-12	RFC 5055 (Proposed Standard)	2
RFC 5272 (draft-ietf-pkix-2797-bis)	Certificate Management over CMS (CMC)	2008-06	RFC 5272 (Proposed Standard) Errata	
RFC 5273 (draft-ietf-pkix-cmc-trans)	Certificate Management over CMS (CMC): Transport Protocols	2008-06	RFC 5273 (Proposed Standard)	
RFC 5274 (draft-ietf-pkix-cmc-compl)	Certificate Management Messages over CMS (CMC): Compliance Requirements	2008-06	RFC 5274 (Proposed Standard)	
RFC 5280 (draft-ietf-pkix-rfc3280bis)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2008-05	RFC 5280 (Proposed Standard) Errata	
RFC 5480 (draft-ietf-pkix-ecc-subpubkeyinfo)	Elliptic Curve Cryptography Subject Public Key Information	2009-03	RFC 5480 (Proposed Standard) Errata	
RFC 5636 (draft-ietf-pkix-tac)	Traceable Anonymous Certificate	2009-08	RFC 5636 (Experimental)	
RFC 5697 (draft-ietf-pkix-other-certs)	Other Certificates Extension	2009-11	RFC 5697 (Experimental)	
RFC 5755 (draft-ietf-pkix-3281update)	An Internet Attribute Certificate Profile for Authorization	2010-01	RFC 5755 (Proposed Standard)	
RFC 5756 (draft-ietf-pkix-rfc4055-update)	Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters	2010-01	RFC 5756 (Proposed Standard) Errata	
RFC 5758 (draft-ietf-pkix-sha2-dsa-ecdsa)	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	2010-01	RFC 5758 (Proposed Standard) Errata	
RFC 5816 (draft-ietf-pkix-rfc3161-update)	ESSCertIDv2 Update for RFC 3161	2010-04	RFC 5816 (Proposed Standard)	
RFC 5877 (draft-ietf-pkix-attr-cert-mime-type)	The application/pkix-attr-cert Media Type for Attribute Certificates	2010-05	RFC 5877 (Informational) Errata	
RFC 5912 (draft-ietf-pkix-new-asn1)	New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)	2010-06	RFC 5912 (Informational) Errata	

Document	Title	Date	Status	Ipr
RFC 5913 (draft-ietf-pkix-authorityclearanceconstraints)	Clearance Attribute and Authority Clearance Constraints Certificate Extension	2010-06	RFC 5913 (Proposed Standard)	
RFC 5914 (draft-ietf-pkix-ta-format)	Trust Anchor Format	2010-06	RFC 5914 (Proposed Standard) Errata	
RFC 5934 (draft-ietf-pkix-tamp)	Trust Anchor Management Protocol (TAMP)	2010-08	RFC 5934 (Proposed Standard) Errata	
RFC 6024 (draft-ietf-pkix-ta-mgmt-reqs)	Trust Anchor Management Requirements	2010-10	RFC 6024 (Informational)	
RFC 6025 (draft-ietf-pkix-asn1-translation)	ASN.1 Translation	2010-10	RFC 6025 (Informational)	
Active Internet-Drafts				
draft-chen-pkix-securityinfo-00	X.509 Extension with Security Information	2010-10-15 expires soon	I-D Exists	
draft-moreau-pkix-aixcm-00	Auto Issued X.509 Certificate Mechanism (AIXCM)	2008-08-06	I-D Exists RFC Editor State: ISR-AUTH	
draft-patterson-pkix-attribute-signing-eku-00	attributeSigning extendedKeyUsage value	2011-03-28	I-D Exists	

Source: http://datatracker.ietf.org/wg/pkix/

IPR Note 1:

draft-ietf-pkix-new-part1, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile":

2001-05-30	ID # 38	"IBM's patent statement pertaining to PKIX, specifically certificateHold for Non-Repudiation"

IPR note 2:

draft-ietf-pkix-scvp, "Server-based Certificate Validation Protocol (SCVP)":

2005-03-25	ID # 563	"CoreStreet, Ltd.'s statement about IPR claimed in draft-ietf-pkix-scvp-18"
2005-06-16	ID # 589	"CoreStreet, Ltd. Statement about IPR claimed in IETF's draft Simple Certificate Validation Protocol - draft-ietf-pkix-scvp-18 ("

5.4 Action Verbs

The following table lists the action verbs used in the requirements along with a definition.

Table 5-3. Requirements Action Verb Definitions

Verb	Definition
accept	receive data into the service/system and consider it to be valid data from a valid source

Verb	Definition
acknowledge	to take notice of, or to recognize as genuine or valid
add	change a configuration or list by creating a new entry
advertise	to make generally or publicly known - does not require both ends of the transmission to have a previously established relationship
be enclosed	refers to the physical environment of the overall system
compare	take two or more parameters or values and analyze them against some determined criteria
conform	refers to the alignment of the system to an external standard - interface, workmanship, operating, etc.
coordinate	exchange information with another entity whereby one entity informs another something about its operation and receives information from the other entity about their operation
correlate	take one or more parameters or values and some determined criteria
create	to fashion or build something new; in the case of the Core System it refers to data or records within a record keeping mechanism
decrypt	decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access
define	to explain the meaning and content of a set of data or a service to a system user or system operator
discard	to remove an item from a collection
display	to present information to a system operator, typically through a graphical user interface or command line prompt
drift	to vary or deviate from a set standard reference
drop	to remove an item from a collection before it has been processed by any higher level services in the system
enable	to make other actions possible by supplying prerequisite information or resources required for the task or activity to take place
encrypt	to encode or change (information) from one form to another especially to hide its meaning in such a way to secure its contents from unauthorized access
establish	to begin or create something that will follow a prescribed set of rules governing the behavior such as an interface between entities.
exceed	to go over a prescribed threshold or parameter
forward	to send data onto another entity (system user) without adding the data to the Core System's set of long term storage

Verb	Definition
generate	to create a message or report that includes elements that could be combined from multiple sources
identify	to extract information from a message or an activity/process that matches certain criteria
implement	to carry out a process or function to a prescribed set of characteristics or constraints
include	to create a message or report that contains certain elements that could be from multiple sources
inform	to present information to a system operator, typically through a graphical user interface or command line prompt, that includes higher level of organization to the presentation beyond a simple display
install	to set up for use or service
interface	to connect by means of an interface or set of connections between entities
log	to make a note or record of : enter details of or about in a log
maintain	to keep in an existing state (as of repair, efficiency, or validity) in order to preserve from failure or decline
manage	to work upon or try to alter for a purpose - involving collecting information and acting on it based on predefined sets of thresholds or criteria
notify	to send a message to another entity that may be sent based on a certain event or intended to cause a certain action on the part of the recipient
operate	describes the conditions in which the Core System is performing its services and functions
perform	to execute a set of processes to achieve a stated purpose and produce prescribed outputs
protect	to carry out certain procedures and setup predefined safeguards in order to maintain the status or integrity of an entity
provide	to supply or make data available (something wanted or needed) to a recipient; may be in a controlled send/receive protocol or by putting information content on a user display
receive	to come into possession of data sent from another entity (source); to be the destination or recipient of data that is transmitted
record	to add information into a set of data (database, log, files) to be organized with other data
report	to create an output either to a System User or a System Operator that is organized to include one or more data elements that could be combined from multiple sources and may be arranged in a prescribed format.

Verb	Definition
request	to send a message to another entity to cause that other entity to reply with data that is called out in the 'request' message
translate	to change from one form or language to another as in a domain name into an Internet Protocol address
respond	to send a message upon stimulation as in a request
restrict	to confine within bounds or to prevent a user from doing something that is not allowed based on their permissions
send	to dispatch by a means of communication data from one entity to another
sign	to apply a digital certificate, or electronic "identification card" that establishes the credentials of the sender of an electronic message.
store	to place or leave in a location (as in computer memory) for preservation or later use or disposal
support	to implement an interface or service in agreement with or in accordance with an external standard definition or established protocol
transition	to change from one state to another
verify	to confirm or substantiate the truth, accuracy, or reality of something - credentials, identity, configuration

5.5 Internal Interfaces

The following table shows the internal interfaces between subsystems within the Core System. The column on the left represents the subsystems that will be sending data to the subsystems represented by the columns to the right.

Table 5-4. Internal Subsystem to Subsystem Interfaces

	Receiving Subsystems							
Sending Subsystems	CC	DD	MM	NS	SM	Time	UP	US
Core2Core (CC)		y	y	y	y		y	y
Data Distribution (DD)	y		y	y	y		y	y
Misbehavior Management (MM)	y				y		y	y
Network Services (NS)	y	y	y		y		y	y
Service Monitor (SM)	y	y	y	y		y	y	y
Time	y	y	y	y	y		y	y
User Permissions (UP)	y	y	y	y	y			y
User Security (US)	y	y	y	y	y		y	

6 Traceability Matrices

This section contains tables that trace the requirements in this document to and from the higher level requirements, in this case it traces to/from the Needs identified in the Core System Concept of Operations (ConOps).

6.1 Needs to Requirements Traceability

6.1.1 Core System Needs to System Requirements Matrix

Table 6-1. Core System Needs to System Requirements Traceability Matrix

	Core System Need	SR ID	SSR ID
1	Data Protection	3.1.1.15	3.2.1.4.4
1	Data Protection	3.1.1.15	3.2.3.1.5.5
1	Data Protection	3.1.1.15	3.2.3.2.3
1	Data Protection	3.1.1.15	3.2.4.1.2.3
1	Data Protection	3.1.1.15	3.2.4.4.1
1	Data Protection	3.1.1.15	3.2.5.1.11.3
1	Data Protection	3.1.1.15	3.2.7.4.1
1	Data Protection	3.1.1.15	3.2.7.4.2
1	Data Protection	3.1.1.15	3.2.7.4.3
1	Data Protection	3.1.1.15	3.2.7.4.4
1	Data Protection	3.1.1.15	3.2.7.4.5
1	Data Protection	3.1.1.15	3.2.7.4.6
1	Data Protection	3.1.1.15	3.2.7.4.7
1	Data Protection	3.1.1.15	3.2.8.1.2.4
1	Data Protection	3.1.1.15	3.2.8.1.2.5
1	Data Protection	3.1.1.15	3.2.8.1.2.6
1	Data Protection	3.1.1.15	3.2.8.1.3.3
1	Data Protection	3.1.1.15	3.2.8.1.3.4
1	Data Protection	3.1.1.15	3.2.8.1.3.5
1	Data Protection	3.1.1.15	3.2.8.4.1
1	Data Protection	3.1.1.15	3.2.8.4.2
1	Data Protection	3.1.1.15	3.2.8.4.3
1	Data Protection	3.1.1.15	3.2.8.4.4
1	Data Protection	3.1.1.15	3.2.8.4.5
1	Data Protection	3.1.1.15	3.2.8.4.6
1	Data Protection	3.1.1.40	3.2.8.1.1.3
1	Data Protection	3.1.1.40	3.2.8.1.1.10
1	Data Protection	3.1.1.40	3.2.8.1.1.4
1	Data Protection	3.1.1.40	3.2.8.1.1.6
1	Data Protection	3.1.1.40	3.2.8.1.1.7
1	Data Protection	3.1.1.40	3.2.8.1.1.8
1	Data Protection	3.1.1.40	3.2.8.1.1.9
1	Data Protection	3.1.1.40	3.2.8.1.1.11
1	Data Protection	3.1.1.40	3.2.8.1.1.12
1	Data Protection	3.1.1.40	3.2.8.1.1.13

	Core System Need	SR ID	SSR ID
1	Data Protection	3.1.1.40	3.2.8.1.1.14
1	Data Protection	3.1.1.40	3.2.8.1.4.23
1	Data Protection	3.1.1.40	3.2.8.1.4.24
1	Data Protection	3.1.1.40	3.2.8.1.4.25
2	Core Trust	3.1.1.9	3.2.1.1.16
2	Core Trust	3.1.1.9	3.2.1.1.17
2	Core Trust	3.1.1.9	3.2.4.1.1.2
2	Core Trust	3.1.1.41	3.2.8.1.1.3
2	Core Trust	3.1.1.41	3.2.8.1.1.4
2	Core Trust	3.1.1.41	3.2.8.1.1.1
2	Core Trust	3.1.1.41	3.2.8.1.4.3
2	Core Trust	3.1.1.41	3.2.8.1.4.6
2	Core Trust	3.1.1.41	3.2.8.1.4.8
2	Core Trust	3.1.1.41	3.2.8.1.4.9
2	Core Trust	3.1.1.41	3.2.8.1.4.19
2	Core Trust	3.1.1.41	3.2.8.1.4.20
2	Core Trust	3.1.1.41	3.2.8.1.4.21
2	Core Trust	3.1.1.41	3.2.8.1.4.22
2	Core Trust	3.1.1.42	3.2.7.3.2.1
2	Core Trust	3.1.1.42	3.2.8.1.1.3
2	Core Trust	3.1.1.42	3.2.8.1.1.4
2	Core Trust	3.1.1.42	3.2.8.1.3.1
2	Core Trust	3.1.1.42	3.2.8.1.3.6
2	Core Trust	3.1.1.42	3.2.8.1.3.7
2	Core Trust	3.1.1.42	3.2.8.1.3.8
2	Core Trust	3.1.1.42	3.2.8.1.3.9
2	Core Trust	3.1.1.42	3.2.8.1.3.12
2	Core Trust	3.1.1.42	3.2.8.1.3.13
2	Core Trust	3.1.1.42	3.2.8.1.3.14
2	Core Trust	3.1.1.42	3.2.8.1.3.15
2	Core Trust	3.1.1.42	3.2.8.1.3.16
2	Core Trust	3.1.1.42	3.2.8.1.3.17
2	Core Trust	3.1.1.42	3.2.8.1.3.18
2	Core Trust	3.1.1.42	3.2.8.1.3.19
2	Core Trust	3.1.1.42	3.2.8.1.3.20
2	Core Trust	3.1.1.42	3.2.8.1.4.3
2	Core Trust	3.1.1.42	3.2.8.1.4.6
2	Core Trust	3.1.1.42	3.2.8.1.4.8
2	Core Trust	3.1.1.42	3.2.8.1.4.9
2	Core Trust	3.1.1.42	3.2.8.3.2.1
2	Core Trust	3.1.1.42	3.2.8.3.2.2
2	Core Trust	3.1.1.43	3.2.8.1.4.1
2	Core Trust	3.1.1.43	3.2.8.1.4.2
2	Core Trust	3.1.1.44	3.2.8.1.1.1
2	Core Trust	3.1.1.44	3.2.8.1.2.1
2	Core Trust	3.1.1.44	3.2.8.1.2.2
2	Core Trust	3.1.1.44	3.2.8.1.2.3

	Core System Need	SR ID	SSR ID
2	Core Trust	3.1.1.44	3.2.8.1.4.1
2	Core Trust	3.1.1.44	3.2.8.1.4.2
2	Core Trust	3.1.1.44	3.2.8.1.4.4
2	Core Trust	3.1.1.44	3.2.8.1.4.7
2	Core Trust	3.1.1.44	3.2.8.1.4.10
2	Core Trust	3.1.1.44	3.2.8.1.4.13
2	Core Trust	3.1.1.44	3.2.8.1.4.16
2	Core Trust	3.1.1.45	3.2.7.3.2.5
2	Core Trust	3.1.1.46	3.2.7.3.2.1
2	Core Trust	3.1.1.46	3.2.8.1.2.10
2	Core Trust	3.1.1.46	3.2.8.1.2.15
2	Core Trust	3.1.1.46	3.2.8.1.2.16
2	Core Trust	3.1.1.46	3.2.8.1.2.17
2	Core Trust	3.1.1.46	3.2.8.1.2.19
2	Core Trust	3.1.1.46	3.2.8.1.2.20
2	Core Trust	3.1.1.46	3.2.8.1.2.8
2	Core Trust	3.1.1.46	3.2.8.3.1.1
2	Core Trust	3.1.2.15	3.2.8.2.1
2	Core Trust	3.1.2.16	3.2.8.2.2
2	Core Trust	3.1.7.2	N/A
2	Core Trust	3.1.7.3	N/A
3	System User Trust	3.1.1.9	3.2.1.1.16
3	System User Trust	3.1.1.9	3.2.1.1.17
3	System User Trust	3.1.1.9	3.2.4.1.1.2
4	Core Trust Revocation	3.1.2.17	3.2.8.1.2.7
4	Core Trust Revocation	3.1.2.17	3.2.8.2.3
4	Core Trust Revocation	3.1.2.18	3.2.8.1.3.6
4	Core Trust Revocation	3.1.2.18	3.2.8.2.4
5	System User Trust Revocation	3.1.2.17	3.2.8.1.2.7
5	System User Trust Revocation	3.1.2.17	3.2.8.2.3
5	System User Trust Revocation	3.1.2.18	3.2.8.1.3.6
5	System User Trust Revocation	3.1.2.18	3.2.8.2.4
6	Authorization Management	3.1.2.12	3.2.7.2.2
6	Authorization Management	3.1.2.14	3.2.7.2.4
6	Authorization Management	3.1.3.6	3.2.7.3.1.1
6	Authorization Management	3.1.3.7	3.2.7.1.2.3
6	Authorization Management	3.1.3.8	3.2.8.3.1.1
6	Authorization Management	3.1.3.9	3.2.8.1.3.2
6	Authorization Management	3.1.4.8	3.2.7.4.2
7	Authorization Verification	3.1.1.19	3.2.1.1.26.4
7	Authorization Verification	3.1.1.19	3.2.2.1.2
7	Authorization Verification	3.1.1.19	3.2.2.1.12
7	Authorization Verification	3.1.1.19	3.2.4.1.1.3
7	Authorization Verification	3.1.1.19	3.2.4.1.1.4
7	Authorization Verification	3.1.1.19	3.2.4.1.1.5
7	Authorization Verification	3.1.1.37	3.2.7.1.1.1
7	Authorization Verification	3.1.1.37	3.2.7.1.2.2

	Core System Need	SR ID	SSR ID
7	Authorization Verification	3.1.1.37	3.2.7.1.2.3
7	Authorization Verification	3.1.1.37	3.2.7.1.2.4
7	Authorization Verification	3.1.1.37	3.2.7.1.2.5
7	Authorization Verification	3.1.1.37	3.2.7.1.2.6
7	Authorization Verification	3.1.1.37	3.2.7.3.1
7	Authorization Verification	3.1.1.37	3.2.7.3.1.2
7	Authorization Verification	3.1.1.37	3.2.7.3.1.3
7	Authorization Verification	3.1.1.37	3.2.7.3.1.4
7	Authorization Verification	3.1.1.38	3.2.7.1.1.2
7	Authorization Verification	3.1.1.38	3.2.7.1.1.3
7	Authorization Verification	3.1.1.38	3.2.7.1.1.4
7	Authorization Verification	3.1.5.1.2	N/A
8	Misbehavior Identification	3.1.1.12	3.2.1.1.24
8	Misbehavior Identification	3.1.1.12	3.2.1.3.2
8	Misbehavior Identification	3.1.1.12	3.2.2.1.17
8	Misbehavior Identification	3.1.1.12	3.2.2.1.18
8	Misbehavior Identification	3.1.1.12	3.2.2.1.19
8	Misbehavior Identification	3.1.1.12	3.2.3.1.1
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.1
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.2
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.3
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.4
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.5
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.6
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.7
8	Misbehavior Identification	3.1.1.12	3.2.3.1.3.8
8	Misbehavior Identification	3.1.1.12	3.2.3.1.5.2
8	Misbehavior Identification	3.1.1.12	3.2.3.1.5.2.1
8	Misbehavior Identification	3.1.1.12	3.2.3.1.5.2.2
8	Misbehavior Identification	3.1.1.12	3.2.3.1.5.3
8	Misbehavior Identification	3.1.1.12	3.2.3.1.5.4
8	Misbehavior Identification	3.1.1.12	3.2.4.1.1.6
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.9
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.10
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.11
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.12
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.13
8	Misbehavior Identification	3.1.1.12	3.2.4.1.3.14
8	Misbehavior Identification	3.1.1.12	3.2.7.1.2.7
8	Misbehavior Identification	3.1.1.12	3.2.7.1.2.8
8	Misbehavior Identification	3.1.1.12	3.2.7.1.2.9
8	Misbehavior Identification	3.1.1.25	3.2.3.1.2.1
8	Misbehavior Identification	3.1.1.25	3.2.3.1.2.3
8	Misbehavior Identification	3.1.1.25	3.2.3.1.4.4
8	Misbehavior Identification	3.1.1.26	3.2.3.1.5.1
8	Misbehavior Identification	3.1.1.27	3.2.1.3.2.4
8	Misbehavior Identification	3.1.1.27	3.2.2.3.2.4

	Core System Need	SR ID	SSR ID
8	Misbehavior Identification	3.1.1.27	3.2.3.1.3.7
8	Misbehavior Identification	3.1.1.27	3.2.3.3.2.2
8	Misbehavior Identification	3.1.2.4	3.2.3.2.1
8	Misbehavior Identification	3.1.2.5	3.2.3.2.2
8	Misbehavior Identification	3.1.3.3	3.2.3.3.1
8	Misbehavior Identification	3.1.3.3	3.2.3.3.2
8	Misbehavior Identification	3.1.4.4	3.2.3.4.1
8	Misbehavior Identification	3.1.4.4	3.2.3.4.2
8	Misbehavior Identification	3.1.4.4	3.2.3.4.3
8	Misbehavior Identification	3.1.4.4	3.2.3.4.4
8	Misbehavior Identification	3.1.4.4	3.2.3.4.5
8	Misbehavior Identification	3.1.4.4	3.2.3.4.6
9	Time Base	3.1.1.24	3.2.1.1.7
9	Time Base	3.1.1.24	3.2.2.1.22.1
9	Time Base	3.1.1.24	3.2.3.1.6.1
9	Time Base	3.1.1.24	3.2.4.1.2.1
9	Time Base	3.1.1.24	3.2.5.1.22
9	Time Base	3.1.1.24	3.2.6.2.1
9	Time Base	3.1.1.24	3.2.6.2.2
9	Time Base	3.1.1.24	3.2.7.1.3.1
9	Time Base	3.1.1.24	3.2.8.1.5.1
9	Time Base	3.1.1.35	3.2.6.1.1
9	Time Base	3.1.1.36	3.2.1.2.1
9	Time Base	3.1.1.36	3.2.6.1.2
9	Time Base	3.1.1.36	3.2.6.1.3
9	Time Base	3.1.1.36	3.2.6.1.5
9	Time Base	3.1.1.36	3.2.6.1.12
9	Time Base	3.1.1.36	3.2.6.2.1
9	Time Base	3.1.1.36	3.2.6.3.1
9	Time Base	3.1.1.36	3.2.6.3.2
9	Time Base	3.1.1.36	3.2.6.3.2.1
9	Time Base	3.1.1.36	3.2.6.3.2.2
9	Time Base	3.1.1.36	3.2.6.3.2.3
9	Time Base	3.1.1.36	3.2.6.3.2.4
9	Time Base	3.1.1.36	3.2.6.3.2.5
9	Time Base	3.1.1.36	3.2.6.3.2.6
9	Time Base	3.1.1.36	3.2.6.3.2.7
9	Time Base	3.1.2.9	3.2.6.2.1
9	Time Base	3.1.2.10	3.2.6.2.1
9	Time Base	3.1.3.5	3.2.6.1.1
10	Data Request	3.1.1.16	3.2.2.1.1.1
10	Data Request	3.1.1.16	3.2.2.1.1.2
10	Data Request	3.1.1.16	3.2.2.1.3
10	Data Request	3.1.1.16	3.2.2.1.3.1
10	Data Request	3.1.1.16	3.2.2.1.3.2
10	Data Request	3.1.1.16	3.2.2.1.4
10	Data Request	3.1.1.16	3.2.2.1.5

	Core System Need	SR ID	SSR ID
10	Data Request	3.1.1.16	3.2.2.4.3
10	Data Request	3.1.1.16	3.2.2.4.4
10	Data Request	3.1.1.16	3.2.2.4.5
10	Data Request	3.1.1.16	3.2.2.4.7
10	Data Request	3.1.3.2	3.2.2.3.2
10	Data Request	3.1.4.3	3.2.2.1.1.1
11	Data Provision	3.1.1.17	3.2.2.1.13.1
11	Data Provision	3.1.1.17	3.2.2.1.20.5
11	Data Provision	3.1.1.17	3.2.2.1.20.6
11	Data Provision	3.1.1.17	3.2.2.4.1
11	Data Provision	3.1.1.17	3.2.2.4.6
11	Data Provision	3.1.1.18	3.2.2.1.6
11	Data Provision	3.1.1.18	3.2.2.1.7
11	Data Provision	3.1.1.18	3.2.2.1.9.1
11	Data Provision	3.1.1.18	3.2.2.1.10
11	Data Provision	3.1.1.18	3.2.2.1.14
11	Data Provision	3.1.1.18	3.2.2.1.21.4
11	Data Provision	3.1.1.18	3.2.2.1.21.7
11	Data Provision	3.1.1.18	3.2.2.3.1
11	Data Provision	3.1.1.18	3.2.2.3.1
11	Data Provision	3.1.1.20	3.2.2.1.1.3
11	Data Provision	3.1.1.20	3.2.2.1.1.4
11	Data Provision	3.1.1.20	3.2.2.1.1.5
11	Data Provision	3.1.1.20	3.2.2.1.1.6
11	Data Provision	3.1.1.20	3.2.2.1.1.7
11	Data Provision	3.1.1.20	3.2.2.1.8.1
11	Data Provision	3.1.1.20	3.2.2.1.10.1
11	Data Provision	3.1.1.20	3.2.2.1.10.2
11	Data Provision	3.1.1.20	3.2.2.1.10.3
11	Data Provision	3.1.1.20	3.2.2.1.10.4
11	Data Provision	3.1.1.20	3.2.2.1.10.5
11	Data Provision	3.1.1.20	3.2.2.1.10.6
11	Data Provision	3.1.1.20	3.2.2.1.10.8
11	Data Provision	3.1.1.20	3.2.2.1.10.9
11	Data Provision	3.1.1.20	3.2.2.1.10.10
11	Data Provision	3.1.1.20	3.2.2.1.11
11	Data Provision	3.1.1.20	3.2.2.1.15
11	Data Provision	3.1.1.20	3.2.2.1.16
11	Data Provision	3.1.1.20	3.2.2.1.20.7
11	Data Provision	3.1.1.20	3.2.2.1.20.8
11	Data Provision	3.1.1.20	3.2.2.1.20.9
11	Data Provision	3.1.1.20	3.2.2.1.20.10
11	Data Provision	3.1.1.20	3.2.2.4.2
11	Data Provision	3.1.1.21	3.2.2.1.20.1
11	Data Provision	3.1.1.21	3.2.2.1.20.2
11	Data Provision	3.1.1.21	3.2.2.1.20.3
11	Data Provision	3.1.1.21	3.2.2.1.20.4

	Core System Need	SR ID	SSR ID
11	Data Provision	3.1.1.22	3.2.2.1.20.11.1
11	Data Provision	3.1.4.2	3.2.2.1.13
11	Data Provision	3.1.4.2	3.2.2.1.13
12	Data Forward	3.1.1.14	3.2.1.1.28
12	Data Forward	3.1.1.14	3.2.1.1.28.1
12	Data Forward	3.1.1.14	3.2.1.1.28.2
12	Data Forward	3.1.1.14	3.2.1.1.28.3
12	Data Forward	3.1.1.14	3.2.1.1.28.4
12	Data Forward	3.1.1.14	3.2.1.4.3
12	Data Forward	3.1.1.14	3.2.2.1.1.8
12	Data Forward	3.1.1.14	3.2.2.1.10.7
12	Data Forward	3.1.1.14	3.2.2.2.1
12	Data Forward	3.1.2.3	3.2.2.2.1
13	Network Connectivity	3.1.3.11	N/A
14	Geographic Broadcast	3.1.1.1	3.2.1.1.1
14	Geographic Broadcast	3.1.1.1	3.2.1.1.2
14	Geographic Broadcast	3.1.1.1	3.2.1.1.3
14	Geographic Broadcast	3.1.1.1	3.2.1.1.4
14	Geographic Broadcast	3.1.1.1	3.2.1.1.5
14	Geographic Broadcast	3.1.1.1	3.2.1.1.29
14	Geographic Broadcast	3.1.1.1	3.2.1.1.29.1
14	Geographic Broadcast	3.1.1.1	3.2.1.1.29.2
14	Geographic Broadcast	3.1.1.1	3.2.1.1.31
14	Geographic Broadcast	3.1.1.1	3.2.1.1.32
14	Geographic Broadcast	3.1.1.1	3.2.1.1.33
14	Geographic Broadcast	3.1.1.1	3.2.2.1.10.8
14	Geographic Broadcast	3.1.1.28	3.2.4.1.1.7
14	Geographic Broadcast	3.1.1.28	3.2.4.1.1.8
14	Geographic Broadcast	3.1.1.28	3.2.4.1.1.9
14	Geographic Broadcast	3.1.1.28	3.2.4.1.2.2
14	Geographic Broadcast	3.1.1.28	3.2.4.1.2.3
14	Geographic Broadcast	3.1.1.28	3.2.4.1.3.1
14	Geographic Broadcast	3.1.1.28	3.2.4.1.3.8
14	Geographic Broadcast	3.1.1.28	3.2.4.1.4
14	Geographic Broadcast	3.1.1.28	3.2.4.1.4.1
14	Geographic Broadcast	3.1.1.28	3.2.4.3.1
14	Geographic Broadcast	3.1.1.28	3.2.4.3.2
14	Geographic Broadcast	3.1.2.6	3.2.4.2.1
14	Geographic Broadcast	3.1.2.7	3.2.4.2.2
14	Geographic Broadcast	3.1.7.6	3.2.1.1.1
15	Core System Service Status	3.1.1.2	3.2.1.1.6
15	Core System Service Status	3.1.1.2	3.2.1.1.30
15	Core System Service Status	3.1.1.2	3.2.2.1.21.5
15	Core System Service Status	3.1.1.2	3.2.3.1.4.5
15	Core System Service Status	3.1.1.2	3.2.4.1.3.2
15	Core System Service Status	3.1.1.2	3.2.5.1.1
15	Core System Service Status	3.1.1.2	3.2.5.1.1.1

	Core System Need	SR ID	SSR ID
15	Core System Service Status	3.1.1.2	3.2.5.1.1.2
15	Core System Service Status	3.1.1.2	3.2.5.1.1.3
15	Core System Service Status	3.1.1.2	3.2.5.1.1.4
15	Core System Service Status	3.1.1.2	3.2.5.1.1.5
15	Core System Service Status	3.1.1.2	3.2.5.1.1.6
15	Core System Service Status	3.1.1.2	3.2.5.1.1.7
15	Core System Service Status	3.1.1.2	3.2.5.1.1.8
15	Core System Service Status	3.1.1.2	3.2.5.1.1.9
15	Core System Service Status	3.1.1.2	3.2.5.1.1.10
15	Core System Service Status	3.1.1.2	3.2.5.1.1.11
15	Core System Service Status	3.1.1.2	3.2.5.1.1.12
15	Core System Service Status	3.1.1.2	3.2.5.1.1.13
15	Core System Service Status	3.1.1.2	3.2.5.1.11.1
15	Core System Service Status	3.1.1.2	3.2.5.1.12.5
15	Core System Service Status	3.1.1.2	3.2.6.1.4
15	Core System Service Status	3.1.1.5	3.2.1.1.10
15	Core System Service Status	3.1.1.5	3.2.2.1.21.8
15	Core System Service Status	3.1.1.5	3.2.3.1.4.7
15	Core System Service Status	3.1.1.5	3.2.4.1.3.4
15	Core System Service Status	3.1.1.5	3.2.5.1.1.15
15	Core System Service Status	3.1.1.5	3.2.5.1.1.16
15	Core System Service Status	3.1.1.5	3.2.5.1.21
15	Core System Service Status	3.1.1.5	3.2.6.1.9
15	Core System Service Status	3.1.1.5	3.2.7.1.2.13
15	Core System Service Status	3.1.1.6	3.2.1.1.11
15	Core System Service Status	3.1.1.6	3.2.2.1.21.2
15	Core System Service Status	3.1.1.6	3.2.3.1.4.2
15	Core System Service Status	3.1.1.6	3.2.4.1.3.6
15	Core System Service Status	3.1.1.6	3.2.5.1.1.14
15	Core System Service Status	3.1.1.6	3.2.5.1.14
15	Core System Service Status	3.1.1.6	3.2.6.1.10
15	Core System Service Status	3.1.1.6	3.2.7.1.2.14
15	Core System Service Status	3.1.1.23	3.2.2.1.21.1
15	Core System Service Status	3.1.1.23	3.2.3.1.4.1
15	Core System Service Status	3.1.1.23	3.2.4.1.3.5
15	Core System Service Status	3.1.1.23	3.2.5.1.8
15	Core System Service Status	3.1.1.23	3.2.5.1.13
15	Core System Service Status	3.1.1.23	3.2.5.1.15
15	Core System Service Status	3.1.1.29	3.2.5.1.1
15	Core System Service Status	3.1.1.29	3.2.5.1.1.1
15	Core System Service Status	3.1.1.29	3.2.5.1.8.1
15	Core System Service Status	3.1.1.31	3.2.5.1.1.18
15	Core System Service Status	3.1.1.31	3.2.5.1.19
15	Core System Service Status	3.1.1.31	3.2.5.2.3
15	Core System Service Status	3.1.1.34	3.2.5.1.9
15	Core System Service Status	3.1.1.34	3.2.5.1.10
15	Core System Service Status	3.1.2.19	N/A

	Core System Need	SR ID	SSR ID
15	Core System Service Status	3.1.3.10	3.2.1.3.2.1
15	Core System Service Status	3.1.3.10	3.2.1.3.2.2
15	Core System Service Status	3.1.3.10	3.2.1.3.2.3
15	Core System Service Status	3.1.3.10	3.2.1.3.2.4
15	Core System Service Status	3.1.3.10	3.2.1.3.2.5
15	Core System Service Status	3.1.3.10	3.2.1.3.2.6
15	Core System Service Status	3.1.3.10	3.2.2.3.2.1
15	Core System Service Status	3.1.3.10	3.2.2.3.2.2
15	Core System Service Status	3.1.3.10	3.2.2.3.2.3
15	Core System Service Status	3.1.3.10	3.2.2.3.2.4
15	Core System Service Status	3.1.3.10	3.2.2.3.2.5
15	Core System Service Status	3.1.3.10	3.2.2.3.2.6
15	Core System Service Status	3.1.3.10	3.2.3.3.2.1
15	Core System Service Status	3.1.3.10	3.2.3.3.2.2
15	Core System Service Status	3.1.3.10	3.2.3.3.2.3
15	Core System Service Status	3.1.3.10	3.2.3.3.2.4
15	Core System Service Status	3.1.3.10	3.2.4.3.2.1
15	Core System Service Status	3.1.3.10	3.2.4.3.2.1
15	Core System Service Status	3.1.3.10	3.2.4.3.2.2
15	Core System Service Status	3.1.3.10	3.2.4.3.2.3
15	Core System Service Status	3.1.3.10	3.2.4.3.2.4
15	Core System Service Status	3.1.3.10	3.2.4.3.2.5
15	Core System Service Status	3.1.3.10	3.2.4.3.2.6
15	Core System Service Status	3.1.3.10	3.2.5.3.2.1
15	Core System Service Status	3.1.3.10	3.2.6.3.2.1
15	Core System Service Status	3.1.3.10	3.2.6.3.2.2
15	Core System Service Status	3.1.3.10	3.2.6.3.2.3
15	Core System Service Status	3.1.3.10	3.2.6.3.2.4
15	Core System Service Status	3.1.3.10	3.2.6.3.2.5
15	Core System Service Status	3.1.3.10	3.2.6.3.2.6
15	Core System Service Status	3.1.3.10	3.2.6.3.2.7
15	Core System Service Status	3.1.3.10	3.2.7.3.2.1
15	Core System Service Status	3.1.3.10	3.2.7.3.2.2
15	Core System Service Status	3.1.3.10	3.2.7.3.2.3
15	Core System Service Status	3.1.3.10	3.2.7.3.2.4
15	Core System Service Status	3.1.3.10	3.2.7.3.2.5
15	Core System Service Status	3.1.3.10	3.2.7.3.2.6
15	Core System Service Status	3.1.3.10	3.2.8.3.2.1
15	Core System Service Status	3.1.3.10	3.2.8.3.2.2
15	Core System Service Status	3.1.3.10	3.2.8.3.2.3
15	Core System Service Status	3.1.3.10	3.2.8.3.2.4
15	Core System Service Status	3.1.3.10	3.2.8.3.2.5
15	Core System Service Status	3.1.3.10	3.2.8.3.2.6
15	Core System Service Status	3.1.4.5	N/A
15	Core System Service Status	3.1.4.6	N/A
15	Core System Service Status	3.1.6.1	N/A
16	System Integrity Protection	3.1.1.4	3.2.1.1.8

	Core System Need	SR ID	SSR ID
16	System Integrity Protection	3.1.1.4	3.2.1.1.9
16	System Integrity Protection	3.1.1.4	3.2.2.1.21.3
16	System Integrity Protection	3.1.1.4	3.2.2.1.21.6
16	System Integrity Protection	3.1.1.4	3.2.3.1.4.3
16	System Integrity Protection	3.1.1.4	3.2.3.1.4.6
16	System Integrity Protection	3.1.1.4	3.2.4.1.3.3
16	System Integrity Protection	3.1.1.4	3.2.4.1.3.7
16	System Integrity Protection	3.1.1.4	3.2.5.1.16
16	System Integrity Protection	3.1.1.4	3.2.5.1.20
16	System Integrity Protection	3.1.1.4	3.2.6.1.6
16	System Integrity Protection	3.1.1.4	3.2.6.1.7
16	System Integrity Protection	3.1.1.4	3.2.6.1.8
16	System Integrity Protection	3.1.1.4	3.2.7.1.2.11
16	System Integrity Protection	3.1.1.4	3.2.7.1.2.12
16	System Integrity Protection	3.1.1.32	3.2.5.1.1.17
16	System Integrity Protection	3.1.1.32	3.2.5.1.11
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.2
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.4
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.5
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.6
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.7
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.8
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.9
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.10
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.11
16	System Integrity Protection	3.1.1.32	3.2.5.1.11.12
16	System Integrity Protection	3.1.1.32	3.2.5.1.12
16	System Integrity Protection	3.1.1.33	3.2.5.1.12.1
16	System Integrity Protection	3.1.1.33	3.2.5.1.12.2
16	System Integrity Protection	3.1.1.33	3.2.5.1.12.3
16	System Integrity Protection	3.1.1.33	3.2.5.1.12.4
16	System Integrity Protection	3.1.2.8	3.2.5.2.1
16	System Integrity Protection	3.1.2.8	3.2.5.2.2
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.1.3.2.6
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.2.3.2.6
16	System Integrity Protection	3.1.3.10	3.2.3.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.3.3.2.2

	Core System Need	SR ID	SSR ID
16	System Integrity Protection	3.1.3.10	3.2.3.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.3.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.4.3.2.6
16	System Integrity Protection	3.1.3.10	3.2.5.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.6
16	System Integrity Protection	3.1.3.10	3.2.6.3.2.7
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.7.3.2.6
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.1
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.2
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.3
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.4
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.5
16	System Integrity Protection	3.1.3.10	3.2.8.3.2.6
16	System Integrity Protection	3.1.5.1.1	N/A
16	System Integrity Protection	3.1.5.1.3	N/A
16	System Integrity Protection	3.1.5.1.4	N/A
16	System Integrity Protection	3.1.5.2.1	N/A
16	System Integrity Protection	3.1.5.2.2	N/A
16	System Integrity Protection	3.1.5.2.3	N/A
16	System Integrity Protection	3.1.5.2.4	N/A
16	System Integrity Protection	3.1.5.2.5	N/A
16	System Integrity Protection	3.1.5.2.6	N/A
16	System Integrity Protection	3.1.5.3.1	N/A
16	System Integrity Protection	3.1.5.3.3	N/A
16	System Integrity Protection	3.1.6.2	N/A
16	System Integrity Protection	3.1.6.3	N/A
16	System Integrity Protection	3.1.6.4	N/A
17	System Availability	3.1.1.13	3.2.1.1.27
17	System Availability	3.1.1.13	3.2.1.1.27.2
17	System Availability	3.1.1.13	3.2.1.1.27.3
17	System Availability	3.1.1.13	3.2.1.1.27.4

	Core System Need	SR ID	SSR ID
17	System Availability	3.1.1.13	3.2.1.1.27.5
17	System Availability	3.1.1.13	3.2.1.1.27.6
17	System Availability	3.1.2.1	3.2.1.3.1
17	System Availability	3.1.5.4.1	N/A
17	System Availability	3.1.5.5.1	N/A
17	System Availability	3.1.5.5.2	N/A
18	System Operational Performance Monitoring	3.1.7.7	N/A
19	Core System Independence	3.1.1.1	3.2.1.1.1
19	Core System Independence	3.1.1.1	3.2.1.1.2
19	Core System Independence	3.1.1.1	3.2.1.1.3
19	Core System Independence	3.1.1.1	3.2.1.1.4
19	Core System Independence	3.1.1.1	3.2.1.1.5
19	Core System Independence	3.1.1.1	3.2.1.1.29
19	Core System Independence	3.1.1.1	3.2.1.1.29.1
19	Core System Independence	3.1.1.1	3.2.1.1.29.2
19	Core System Independence	3.1.1.1	3.2.1.1.31
19	Core System Independence	3.1.1.1	3.2.1.1.32
19	Core System Independence	3.1.1.1	3.2.1.1.33
19	Core System Independence	3.1.1.1	3.2.2.1.10.8
19	Core System Independence	3.1.1.11	3.2.1.1.15
19	Core System Independence	3.1.1.11	3.2.1.1.22
19	Core System Independence	3.1.1.11	3.2.5.1.2
19	Core System Independence	3.1.1.11	3.2.5.1.3
19	Core System Independence	3.1.1.11	3.2.5.1.4
19	Core System Independence	3.1.1.11	3.2.5.1.5
19	Core System Independence	3.1.1.11	3.2.5.1.6
19	Core System Independence	3.1.1.11	3.2.5.1.7
19	Core System Independence	3.1.1.11	3.2.5.1.17
19	Core System Independence	3.1.1.11	3.2.5.1.18
19	Core System Independence	3.1.1.11	3.2.5.2.4
19	Core System Independence	3.1.1.30	3.2.1.1.22
19	Core System Independence	3.1.3.4	3.2.5.3.1
19	Core System Independence	3.1.3.4	3.2.5.3.2
19	Core System Independence	3.1.7.9	3.2.4.1.1.1
20	Core System Interoperability	3.1.1.7	3.2.1.1.12
20	Core System Interoperability	3.1.1.7	3.2.1.1.13
20	Core System Interoperability	3.1.1.7	3.2.1.1.14
20	Core System Interoperability	3.1.1.7	3.2.1.1.20
20	Core System Interoperability	3.1.1.7	3.2.1.1.21
20	Core System Interoperability	3.1.1.7	3.2.1.1.27.7
20	Core System Interoperability	3.1.1.7	3.2.1.1.27.8
20	Core System Interoperability	3.1.1.8	3.2.1.1.31
20	Core System Interoperability	3.1.1.8	3.2.1.1.32
20	Core System Interoperability	3.1.1.8	3.2.1.1.33
20	Core System Interoperability	3.1.3.1	3.2.1.1.16
20	Core System Interoperability	3.1.3.1	3.2.1.1.26

	Core System Need	SR ID	SSR ID
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.1
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.2
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.3
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.4
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.5
20	Core System Interoperability	3.1.3.1	3.2.1.3.2.6
20	Core System Interoperability	3.1.3.1	3.2.2.3.2.1
20	Core System Interoperability	3.1.3.1	3.2.3.3.2.1
20	Core System Interoperability	3.1.3.1	3.2.5.3.2.1
20	Core System Interoperability	3.1.3.1	3.2.7.3.2.1
20	Core System Interoperability	3.1.3.1	3.2.7.3.2.2
20	Core System Interoperability	3.1.3.1	3.2.8.3.2.1
20	Core System Interoperability	3.1.7.4	N/A
21	Core System Interdependence	3.1.2.2	3.2.1.2.2
21	Core System Interdependence	3.1.2.11	3.2.7.2.1
21	Core System Interdependence	3.1.2.13	3.2.7.2.3
21	Core System Interdependence	3.1.3.1	3.2.1.1.16
21	Core System Interdependence	3.1.3.1	3.2.1.1.26
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.1
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.2
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.3
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.4
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.5
21	Core System Interdependence	3.1.3.1	3.2.1.3.2.6
21	Core System Interdependence	3.1.3.1	3.2.2.3.2.1
21	Core System Interdependence	3.1.3.1	3.2.3.3.2.1
21	Core System Interdependence	3.1.3.1	3.2.5.3.2.1
21	Core System Interdependence	3.1.3.1	3.2.7.3.2.1
21	Core System Interdependence	3.1.3.1	3.2.7.3.2.2
21	Core System Interdependence	3.1.3.1	3.2.8.3.2.1
21	Core System Interdependence	3.1.4.1	3.2.1.1.22
21	Core System Interdependence	3.1.4.1	3.2.1.1.23
21	Core System Interdependence	3.1.4.1	3.2.1.1.24
21	Core System Interdependence	3.1.4.1	3.2.1.1.25
21	Core System Interdependence	3.1.4.1	3.2.1.1.25.1
21	Core System Interdependence	3.1.4.1	3.2.1.1.26
21	Core System Interdependence	3.1.4.1	3.2.1.1.26.1
21	Core System Interdependence	3.1.4.1	3.2.1.1.26.2
21	Core System Interdependence	3.1.4.1	3.2.1.1.26.3
21	Core System Interdependence	3.1.4.1	3.2.1.1.27.1
21	Core System Interdependence	3.1.4.1	3.2.1.2.1
21	Core System Interdependence	3.1.4.1	3.2.1.4.1
21	Core System Interdependence	3.1.4.1	3.2.1.4.2
22	Core System Data Protection	3.1.1.10	3.2.1.1.18
22	Core System Data Protection	3.1.1.10	3.2.1.1.19
22	Core System Data Protection	3.1.1.15	3.2.1.4.4
22	Core System Data Protection	3.1.1.15	3.2.3.1.5.5

	Core System Need	SR ID	SSR ID
22	Core System Data Protection	3.1.1.15	3.2.3.2.3
22	Core System Data Protection	3.1.1.15	3.2.4.1.2.3
22	Core System Data Protection	3.1.1.15	3.2.4.4.1
22	Core System Data Protection	3.1.1.15	3.2.5.1.11.3
22	Core System Data Protection	3.1.1.15	3.2.7.4.1
22	Core System Data Protection	3.1.1.15	3.2.7.4.2
22	Core System Data Protection	3.1.1.15	3.2.7.4.3
22	Core System Data Protection	3.1.1.15	3.2.7.4.4
22	Core System Data Protection	3.1.1.15	3.2.7.4.5
22	Core System Data Protection	3.1.1.15	3.2.7.4.6
22	Core System Data Protection	3.1.1.15	3.2.7.4.7
22	Core System Data Protection	3.1.1.15	3.2.8.1.2.4
22	Core System Data Protection	3.1.1.15	3.2.8.1.2.5
22	Core System Data Protection	3.1.1.15	3.2.8.1.2.6
22	Core System Data Protection	3.1.1.15	3.2.8.1.3.3
22	Core System Data Protection	3.1.1.15	3.2.8.1.3.4
22	Core System Data Protection	3.1.1.15	3.2.8.1.3.5
22	Core System Data Protection	3.1.1.15	3.2.8.4.1
22	Core System Data Protection	3.1.1.15	3.2.8.4.2
22	Core System Data Protection	3.1.1.15	3.2.8.4.3
22	Core System Data Protection	3.1.1.15	3.2.8.4.4
22	Core System Data Protection	3.1.1.15	3.2.8.4.5
22	Core System Data Protection	3.1.1.15	3.2.8.4.6
22	Core System Data Protection	3.1.4.7	N/A
22	Core System Data Protection	3.1.4.8	3.2.7.4.2
22	Core System Data Protection	3.1.4.9	3.2.8.1.2.5
22	Core System Data Protection	3.1.4.9	3.2.8.1.3.4
22	Core System Data Protection	3.1.4.10	3.2.8.1.2.13
22	Core System Data Protection	3.1.4.10	3.2.8.1.2.14
22	Core System Data Protection	3.1.4.10	3.2.8.1.2.18
22	Core System Data Protection	3.1.4.10	3.2.8.1.2.9
22	Core System Data Protection	3.1.4.10	3.2.8.1.4.17
22	Core System Data Protection	3.1.4.10	3.2.8.1.4.18
23	Anonymity Preservation	3.1.7.1	N/A

6.1.2 System Requirements to Core System Needs Matrix

Table 6-2. System Requirements to Core System Needs Traceability

SR ID		Core System Need
3.1.1.1	14	Geographic Broadcast
3.1.1.1	19	Core System Independence
3.1.1.2	15	Core System Service Status
3.1.1.4	16	System Integrity Protection
3.1.1.5	15	Core System Service Status
3.1.1.6	15	Core System Service Status
3.1.1.7	20	Core System Interoperability
3.1.1.8	20	Core System Interoperability

SR ID		Core System Need
3.1.1.9	2	Core Trust
3.1.1.9	3	System User Trust
3.1.1.10	22	Core System Data Protection
3.1.1.11	19	Core System Independence
3.1.1.12	8	Misbehavior Identification
3.1.1.13	17	System Availability
3.1.1.14	12	Data Forward
3.1.1.15	1	Data Protection
3.1.1.15	22	Core System Data Protection
3.1.1.16	10	Data Request
3.1.1.17	11	Data Provision
3.1.1.18	11	Data Provision
3.1.1.19	7	Authorization Verification
3.1.1.20	11	Data Provision
3.1.1.21	11	Data Provision
3.1.1.22	11	Data Provision
3.1.1.23	15	Core System Service Status
3.1.1.24	9	Time Base
3.1.1.25	8	Misbehavior Identification
3.1.1.26	8	Misbehavior Identification
3.1.1.27	8	Misbehavior Identification
3.1.1.28	14	Geographic Broadcast
3.1.1.29	15	Core System Service Status
3.1.1.30	19	Core System Independence
3.1.1.31	15	Core System Service Status
3.1.1.32	16	System Integrity Protection
3.1.1.33	16	System Integrity Protection
3.1.1.34	15	Core System Service Status
3.1.1.35	9	Time Base
3.1.1.36	9	Time Base
3.1.1.37	7	Authorization Verification
3.1.1.38	7	Authorization Verification
3.1.1.40	1	Data Protection
3.1.1.41	2	Core Trust
3.1.1.42	2	Core Trust
3.1.1.43	2	Core Trust
3.1.1.44	2	Core Trust
3.1.1.45	2	Core Trust
3.1.1.46	2	Core Trust
3.1.2.1	17	System Availability
3.1.2.2	21	Core System Interdependence
3.1.2.3	12	Data Forward
3.1.2.4	8	Misbehavior Identification
3.1.2.5	8	Misbehavior Identification
3.1.2.6	14	Geographic Broadcast
3.1.2.7	14	Geographic Broadcast
3.1.2.8	16	System Integrity Protection
3.1.2.9	9	Time Base
3.1.2.10	9	Time Base

SR ID		Core System Need
3.1.2.11	21	Core System Interdependence
3.1.2.12	6	Authorization Management
3.1.2.13	21	Core System Interdependence
3.1.2.14	6	Authorization Management
3.1.2.15	2	Core Trust
3.1.2.16	2	Core Trust
3.1.2.17	4	Core Trust Revocation
3.1.2.17	5	System User Trust Revocation
3.1.2.18	4	Core Trust Revocation
3.1.2.18	5	System User Trust Revocation
3.1.2.19	15	Core System Service Status
3.1.3.1	20	Core System Interoperability
3.1.3.1	21	Core System Interdependence
3.1.3.2	10	Data Request
3.1.3.3	8	Misbehavior Identification
3.1.3.4	19	Core System Independence
3.1.3.5	9	Time Base
3.1.3.6	6	Authorization Management
3.1.3.7	6	Authorization Management
3.1.3.8	6	Authorization Management
3.1.3.9	6	Authorization Management
3.1.3.10	15	Core System Service Status
3.1.3.10	16	System Integrity Protection
3.1.3.11	13	Network Connectivity
3.1.4.1	21	Core System Interdependence
3.1.4.2	11	Data Provision
3.1.4.2	11	Data Provision
3.1.4.3	10	Data Request
3.1.4.4	8	Misbehavior Identification
3.1.4.5	15	Core System Service Status
3.1.4.6	15	Core System Service Status
3.1.4.7	22	Core System Data Protection
3.1.4.8	6	Authorization Management
3.1.4.8	22	Core System Data Protection
3.1.4.9	22	Core System Data Protection
3.1.4.10	22	Core System Data Protection
3.1.5.1.1	16	System Integrity Protection
3.1.5.1.2	7	Authorization Verification
3.1.5.1.3	16	System Integrity Protection
3.1.5.1.4	16	System Integrity Protection
3.1.5.2.1	16	System Integrity Protection
3.1.5.2.2	16	System Integrity Protection
3.1.5.2.3	16	System Integrity Protection
3.1.5.2.4	16	System Integrity Protection
3.1.5.2.5	16	System Integrity Protection
3.1.5.2.6	16	System Integrity Protection
3.1.5.3.1	16	System Integrity Protection
3.1.5.3.3	16	System Integrity Protection
3.1.5.4.1	17	System Availability

SR ID		Core System Need
3.1.5.5.1	17	System Availability
3.1.5.5.2	17	System Availability
3.1.6.1	15	Core System Service Status
3.1.6.2	16	System Integrity Protection
3.1.6.3	16	System Integrity Protection
3.1.6.4	16	System Integrity Protection
3.1.7.1	23	Anonymity Preservation
3.1.7.2	2	Core Trust
3.1.7.3	2	Core Trust
3.1.7.4	20	Core System Interoperability
3.1.7.5	19	Core System Independence
3.1.7.6	14	Geographic Broadcast
3.1.7.7	18	System Operational Performance Monitoring
3.1.7.8	19	Core System Independence
3.1.7.9	19	Core System Independence

6.1.3 Subsystem to System Matrix

Table 6-3. Subsystem Requirements (SSR) to System Requirements (SR) Traceability

SSR ID	SR ID
3.2.1.1.1	3.1.1.1
3.2.1.1.1	3.1.7.6
3.2.1.1.2	3.1.1.1
3.2.1.1.3	3.1.1.1
3.2.1.1.4	3.1.1.1
3.2.1.1.5	3.1.1.1
3.2.1.1.6	3.1.1.2
3.2.1.1.7	3.1.1.24
3.2.1.1.8	3.1.1.4
3.2.1.1.9	3.1.1.4
3.2.1.1.10	3.1.1.5
3.2.1.1.11	3.1.1.6
3.2.1.1.12	3.1.1.7
3.2.1.1.13	3.1.1.7
3.2.1.1.14	3.1.1.7
3.2.1.1.15	3.1.1.11
3.2.1.1.16	3.1.1.9
3.2.1.1.16	3.1.1.39
3.2.1.1.16	3.1.3.1
3.2.1.1.17	3.1.1.9
3.2.1.1.17	3.1.1.39
3.2.1.1.18	3.1.1.10
3.2.1.1.19	3.1.1.10
3.2.1.1.20	3.1.1.7
3.2.1.1.21	3.1.1.7
3.2.1.1.22	3.1.1.11
3.2.1.1.22	3.1.1.30
3.2.1.1.22	3.1.4.1
3.2.1.1.23	3.1.4.1
3.2.1.1.24	3.1.1.12
3.2.1.1.24	3.1.4.1
3.2.1.1.25	3.1.4.1
3.2.1.1.25.1	3.1.4.1
3.2.1.1.26	3.1.3.1
3.2.1.1.26	3.1.4.1
3.2.1.1.26.1	3.1.4.1
3.2.1.1.26.2	3.1.4.1
3.2.1.1.26.3	3.1.4.1
3.2.1.1.26.4	3.1.1.19
3.2.1.1.26.4	3.1.1.39
3.2.1.1.27	3.1.1.13
3.2.1.1.27.1	3.1.4.1
3.2.1.1.27.2	3.1.1.13
3.2.1.1.27.3	3.1.1.13
3.2.1.1.27.4	3.1.1.13
3.2.1.1.27.5	3.1.1.13
3.2.1.1.27.6	3.1.1.13
3.2.1.1.27.7	3.1.1.7
3.2.1.1.27.8	3.1.1.7
3.2.1.1.28	3.1.1.14
3.2.1.1.28.1	3.1.1.14
3.2.1.1.28.2	3.1.1.14
3.2.1.1.28.3	3.1.1.14
3.2.1.1.28.4	3.1.1.14
3.2.1.1.29	3.1.1.1
3.2.1.1.29.1	3.1.1.1
3.2.1.1.29.2	3.1.1.1
3.2.1.1.30	3.1.1.2
3.2.1.1.31	3.1.1.1
3.2.1.1.31	3.1.1.8
3.2.1.1.32	3.1.1.1
3.2.1.1.32	3.1.1.8
3.2.1.1.33	3.1.1.1
3.2.1.1.33	3.1.1.8
3.2.1.2.1	3.1.1.36
3.2.1.2.1	3.1.4.1
3.2.1.2.2	3.1.2.2
3.2.1.3.1	3.1.2.1
3.2.1.3.2	3.1.1.12
3.2.1.3.2.1	3.1.3.1
3.2.1.3.2.1	3.1.3.10
3.2.1.3.2.2	3.1.3.1
3.2.1.3.2.2	3.1.3.10
3.2.1.3.2.3	3.1.3.1
3.2.1.3.2.3	3.1.3.10
3.2.1.3.2.4	3.1.1.27
3.2.1.3.2.4	3.1.3.1
3.2.1.3.2.4	3.1.3.10
3.2.1.3.2.5	3.1.3.1
3.2.1.3.2.5	3.1.3.10
3.2.1.3.2.6	3.1.3.1
3.2.1.3.2.6	3.1.3.10
3.2.1.4.1	3.1.4.1
3.2.1.4.2	3.1.4.1
3.2.1.4.3	3.1.1.14
3.2.1.4.4	3.1.1.15
3.2.2.1.1.1	3.1.1.16
3.2.2.1.1.1	3.1.4.3
3.2.2.1.1.2	3.1.1.16
3.2.2.1.1.3	3.1.1.20
3.2.2.1.1.4	3.1.1.20
3.2.2.1.1.5	3.1.1.20
3.2.2.1.1.6	3.1.1.20
3.2.2.1.1.7	3.1.1.20
3.2.2.1.1.8	3.1.1.14
3.2.2.1.2	3.1.1.19
3.2.2.1.3	3.1.1.16
3.2.2.1.3.1	3.1.1.16
3.2.2.1.3.2	3.1.1.16
3.2.2.1.4	3.1.1.16
3.2.2.1.5	3.1.1.16
3.2.2.1.6	3.1.1.18
3.2.2.1.7	3.1.1.18
3.2.2.1.8.1	3.1.1.20
3.2.2.1.9.1	3.1.1.18
3.2.2.1.10	3.1.1.18
3.2.2.1.10.1	3.1.1.20
3.2.2.1.10.2	3.1.1.20
3.2.2.1.10.3	3.1.1.20
3.2.2.1.10.4	3.1.1.20
3.2.2.1.10.5	3.1.1.20
3.2.2.1.10.6	3.1.1.20
3.2.2.1.10.7	3.1.1.14
3.2.2.1.10.8	3.1.1.1
3.2.2.1.10.8	3.1.1.20
3.2.2.1.10.9	3.1.1.20
3.2.2.1.10.10	3.1.1.20
3.2.2.1.11	3.1.1.20
3.2.2.1.12	3.1.1.19
3.2.2.1.13	3.1.4.2
3.2.2.1.13.1	3.1.1.17
3.2.2.1.14	3.1.1.18
3.2.2.1.15	3.1.1.20
3.2.2.1.16	3.1.1.20
3.2.2.1.17	3.1.1.12
3.2.2.1.18	3.1.1.12
3.2.2.1.19	3.1.1.12
3.2.2.1.20.1	3.1.1.21
3.2.2.1.20.2	3.1.1.21

SSR ID	SR ID
3.2.2.1.20.3	3.1.1.21
3.2.2.1.20.4	3.1.1.21
3.2.2.1.20.5	3.1.1.17
3.2.2.1.20.6	3.1.1.17
3.2.2.1.20.7	3.1.1.20
3.2.2.1.20.8	3.1.1.20
3.2.2.1.20.9	3.1.1.20
3.2.2.1.20.10	3.1.1.20
3.2.2.1.20.11.1	3.1.1.22
3.2.2.1.21.1	3.1.1.23
3.2.2.1.21.2	3.1.1.6
3.2.2.1.21.3	3.1.1.4
3.2.2.1.21.4	3.1.1.18
3.2.2.1.21.5	3.1.1.2
3.2.2.1.21.6	3.1.1.4
3.2.2.1.21.7	3.1.1.18
3.2.2.1.21.8	3.1.1.5
3.2.2.1.22.1	3.1.1.24
3.2.2.2.1	3.1.1.14
3.2.2.2.1	3.1.2.3
3.2.2.3.1	3.1.1.18
3.2.2.3.1	3.1.1.18
3.2.2.3.2	3.1.3.2
3.2.2.3.2.1	3.1.3.1
3.2.2.3.2.1	3.1.3.10
3.2.2.3.2.2	3.1.3.10
3.2.2.3.2.3	3.1.3.10
3.2.2.3.2.4	3.1.1.27
3.2.2.3.2.4	3.1.3.10
3.2.2.3.2.5	3.1.3.10
3.2.2.3.2.6	3.1.3.10
3.2.2.4.1	3.1.1.17
3.2.2.4.2	3.1.1.20
3.2.2.4.3	3.1.1.16
3.2.2.4.4	3.1.1.16
3.2.2.4.5	3.1.1.16
3.2.2.4.6	3.1.1.17
3.2.2.4.7	3.1.1.16
3.2.3.1.1	3.1.1.12
3.2.3.1.2.1	3.1.1.25
3.2.3.1.2.3	3.1.1.25
3.2.3.1.3.1	3.1.1.12
3.2.3.1.3.2	3.1.1.12
3.2.3.1.3.3	3.1.1.12
3.2.3.1.3.4	3.1.1.12
3.2.3.1.3.5	3.1.1.12
3.2.3.1.3.6	3.1.1.12

SSR ID	SR ID
3.2.3.1.3.7	3.1.1.12
3.2.3.1.3.7	3.1.1.27
3.2.3.1.3.8	3.1.1.12
3.2.3.1.4.1	3.1.1.23
3.2.3.1.4.2	3.1.1.6
3.2.3.1.4.3	3.1.1.4
3.2.3.1.4.4	3.1.1.25
3.2.3.1.4.5	3.1.1.2
3.2.3.1.4.6	3.1.1.4
3.2.3.1.4.7	3.1.1.5
3.2.3.1.5.1	3.1.1.26
3.2.3.1.5.2	3.1.1.12
3.2.3.1.5.2.1	3.1.1.12
3.2.3.1.5.2.2	3.1.1.12
3.2.3.1.5.3	3.1.1.12
3.2.3.1.5.4	3.1.1.12
3.2.3.1.5.5	3.1.1.15
3.2.3.1.6.1	3.1.1.24
3.2.3.2.1	3.1.2.4
3.2.3.2.2	3.1.2.5
3.2.3.2.3	3.1.1.15
3.2.3.3.1	3.1.3.3
3.2.3.3.2	3.1.3.3
3.2.3.3.2.1	3.1.3.1
3.2.3.3.2.1	3.1.3.10
3.2.3.3.2.2	3.1.1.27
3.2.3.3.2.2	3.1.3.10
3.2.3.3.2.3	3.1.3.10
3.2.3.3.2.4	3.1.3.10
3.2.3.4.1	3.1.4.4
3.2.3.4.2	3.1.4.4
3.2.3.4.3	3.1.4.4
3.2.3.4.4	3.1.4.4
3.2.3.4.5	3.1.4.4
3.2.3.4.6	3.1.4.4
3.2.4.1.1.1	3.1.7.9
3.2.4.1.1.2	3.1.1.9
3.2.4.1.1.2	3.1.1.39
3.2.4.1.1.3	3.1.1.19
3.2.4.1.1.4	3.1.1.19
3.2.4.1.1.5	3.1.1.19
3.2.4.1.1.6	3.1.1.12
3.2.4.1.1.7	3.1.1.28
3.2.4.1.1.8	3.1.1.28
3.2.4.1.1.9	3.1.1.28
3.2.4.1.2.1	3.1.1.24
3.2.4.1.2.2	3.1.1.28

SSR ID	SR ID
3.2.4.1.2.3	3.1.1.15
3.2.4.1.2.3	3.1.1.28
3.2.4.1.3.1	3.1.1.28
3.2.4.1.3.2	3.1.1.2
3.2.4.1.3.3	3.1.1.4
3.2.4.1.3.4	3.1.1.5
3.2.4.1.3.5	3.1.1.23
3.2.4.1.3.6	3.1.1.6
3.2.4.1.3.7	3.1.1.4
3.2.4.1.3.8	3.1.1.28
3.2.4.1.3.9	3.1.1.12
3.2.4.1.3.10	3.1.1.12
3.2.4.1.3.11	3.1.1.12
3.2.4.1.3.12	3.1.1.12
3.2.4.1.3.13	3.1.1.12
3.2.4.1.3.14	3.1.1.12
3.2.4.1.4	3.1.1.28
3.2.4.1.4.1	3.1.1.28
3.2.4.2.1	3.1.2.6
3.2.4.2.2	3.1.2.7
3.2.4.3.1	3.1.1.28
3.2.4.3.2	3.1.1.28
3.2.4.3.2.1	3.1.3.10
3.2.4.3.2.1	3.1.3.10
3.2.4.3.2.2	3.1.3.10
3.2.4.3.2.3	3.1.3.10
3.2.4.3.2.4	3.1.3.10
3.2.4.3.2.5	3.1.3.10
3.2.4.3.2.6	3.1.3.10
3.2.4.4.1	3.1.1.15
3.2.5.1.1	3.1.1.2
3.2.5.1.1	3.1.1.29
3.2.5.1.1.1	3.1.1.2
3.2.5.1.1.1	3.1.1.29
3.2.5.1.1.2	3.1.1.2
3.2.5.1.1.3	3.1.1.2
3.2.5.1.1.4	3.1.1.2
3.2.5.1.1.5	3.1.1.2
3.2.5.1.1.6	3.1.1.2
3.2.5.1.1.7	3.1.1.2
3.2.5.1.1.8	3.1.1.2
3.2.5.1.1.9	3.1.1.2
3.2.5.1.1.10	3.1.1.2
3.2.5.1.1.11	3.1.1.2
3.2.5.1.1.12	3.1.1.2
3.2.5.1.1.13	3.1.1.2
3.2.5.1.1.14	3.1.1.6

SSR ID	SR ID
3.2.5.1.1.15	3.1.1.5
3.2.5.1.1.16	3.1.1.5
3.2.5.1.1.17	3.1.1.32
3.2.5.1.1.18	3.1.1.31
3.2.5.1.2	3.1.1.11
3.2.5.1.3	3.1.1.11
3.2.5.1.4	3.1.1.11
3.2.5.1.5	3.1.1.11
3.2.5.1.6	3.1.1.11
3.2.5.1.7	3.1.1.11
3.2.5.1.8	3.1.1.23
3.2.5.1.8.1	3.1.1.29
3.2.5.1.9	3.1.1.34
3.2.5.1.10	3.1.1.34
3.2.5.1.11	3.1.1.32
3.2.5.1.11.1	3.1.1.2
3.2.5.1.11.2	3.1.1.32
3.2.5.1.11.3	3.1.1.15
3.2.5.1.11.4	3.1.1.32
3.2.5.1.11.5	3.1.1.32
3.2.5.1.11.6	3.1.1.32
3.2.5.1.11.7	3.1.1.32
3.2.5.1.11.8	3.1.1.32
3.2.5.1.11.9	3.1.1.32
3.2.5.1.11.10	3.1.1.32
3.2.5.1.11.11	3.1.1.32
3.2.5.1.11.12	3.1.1.32
3.2.5.1.12	3.1.1.32
3.2.5.1.12.1	3.1.1.33
3.2.5.1.12.2	3.1.1.33
3.2.5.1.12.3	3.1.1.33
3.2.5.1.12.4	3.1.1.33
3.2.5.1.12.5	3.1.1.2
3.2.5.1.13	3.1.1.23
3.2.5.1.14	3.1.1.6
3.2.5.1.15	3.1.1.23
3.2.5.1.16	3.1.1.4
3.2.5.1.17	3.1.1.11
3.2.5.1.18	3.1.1.11
3.2.5.1.19	3.1.1.31
3.2.5.1.20	3.1.1.4
3.2.5.1.21	3.1.1.5
3.2.5.1.22	3.1.1.24
3.2.5.2.1	3.1.2.8
3.2.5.2.2	3.1.2.8
3.2.5.2.3	3.1.1.31
3.2.5.2.4	3.1.1.11

SSR ID	SR ID
3.2.5.3.1	3.1.3.4
3.2.5.3.2	3.1.3.4
3.2.5.3.2.1	3.1.3.1
3.2.5.3.2.1	3.1.3.10
3.2.6.1.1	3.1.1.35
3.2.6.1.1	3.1.3.5
3.2.6.1.2	3.1.1.36
3.2.6.1.3	3.1.1.36
3.2.6.1.4	3.1.1.2
3.2.6.1.5	3.1.1.36
3.2.6.1.6	3.1.1.4
3.2.6.1.7	3.1.1.4
3.2.6.1.8	3.1.1.4
3.2.6.1.9	3.1.1.5
3.2.6.1.10	3.1.1.6
3.2.6.1.12	3.1.1.36
3.2.6.2.1	3.1.1.24
3.2.6.2.1	3.1.1.36
3.2.6.2.1	3.1.2.9
3.2.6.2.1	3.1.2.10
3.2.6.2.2	3.1.1.24
3.2.6.3.1	3.1.1.36
3.2.6.3.2	3.1.1.36
3.2.6.3.2.1	3.1.1.36
3.2.6.3.2.1	3.1.3.10
3.2.6.3.2.2	3.1.1.36
3.2.6.3.2.2	3.1.3.10
3.2.6.3.2.3	3.1.1.36
3.2.6.3.2.3	3.1.3.10
3.2.6.3.2.4	3.1.1.36
3.2.6.3.2.4	3.1.3.10
3.2.6.3.2.5	3.1.1.36
3.2.6.3.2.5	3.1.3.10
3.2.6.3.2.6	3.1.1.36
3.2.6.3.2.6	3.1.3.10
3.2.6.3.2.7	3.1.1.36
3.2.6.3.2.7	3.1.3.10
3.2.7.1.1.1	3.1.1.37
3.2.7.1.1.2	3.1.1.38
3.2.7.1.1.3	3.1.1.38
3.2.7.1.1.4	3.1.1.38
3.2.7.1.2.1	3.1.1.39
3.2.7.1.2.2	3.1.1.37
3.2.7.1.2.3	3.1.1.37
3.2.7.1.2.3	3.1.3.7
3.2.7.1.2.4	3.1.1.37
3.2.7.1.2.5	3.1.1.37

SSR ID	SR ID
3.2.7.1.2.6	3.1.1.37
3.2.7.1.2.7	3.1.1.12
3.2.7.1.2.8	3.1.1.12
3.2.7.1.2.9	3.1.1.12
3.2.7.1.2.10	3.1.1.39
3.2.7.1.2.11	3.1.1.4
3.2.7.1.2.12	3.1.1.4
3.2.7.1.2.13	3.1.1.5
3.2.7.1.2.14	3.1.1.6
3.2.7.1.3.1	3.1.1.24
3.2.7.2.1	3.1.2.11
3.2.7.2.2	3.1.2.12
3.2.7.2.3	3.1.2.13
3.2.7.2.4	3.1.2.14
3.2.7.3.1	3.1.1.37
3.2.7.3.1.1	3.1.3.6
3.2.7.3.1.2	3.1.1.37
3.2.7.3.1.3	3.1.1.37
3.2.7.3.1.4	3.1.1.37
3.2.7.3.2	3.1.1.39
3.2.7.3.2.1	3.1.1.42
3.2.7.3.2.1	3.1.1.46
3.2.7.3.2.1	3.1.3.1
3.2.7.3.2.1	3.1.3.10
3.2.7.3.2.2	3.1.1.39
3.2.7.3.2.2	3.1.3.1
3.2.7.3.2.2	3.1.3.10
3.2.7.3.2.3	3.1.1.39
3.2.7.3.2.3	3.1.3.10
3.2.7.3.2.4	3.1.1.39
3.2.7.3.2.4	3.1.3.10
3.2.7.3.2.5	3.1.1.45
3.2.7.3.2.5	3.1.3.10
3.2.7.3.2.6	3.1.1.39
3.2.7.3.2.6	3.1.3.10
3.2.7.4.1	3.1.1.15
3.2.7.4.2	3.1.1.15
3.2.7.4.2	3.1.4.8
3.2.7.4.3	3.1.1.15
3.2.7.4.4	3.1.1.15
3.2.7.4.5	3.1.1.15
3.2.7.4.6	3.1.1.15
3.2.7.4.7	3.1.1.15
3.2.8.1.1.3	3.1.1.40
3.2.8.1.1.3	3.1.1.41
3.2.8.1.1.3	3.1.1.42
3.2.8.1.1.10	3.1.1.40

SSR ID	SR ID
3.2.8.1.1.4	3.1.1.40
3.2.8.1.1.4	3.1.1.41
3.2.8.1.1.4	3.1.1.42
3.2.8.1.1.5	3.1.1.39
3.2.8.1.1.6	3.1.1.40
3.2.8.1.1.7	3.1.1.40
3.2.8.1.1.8	3.1.1.40
3.2.8.1.1.9	3.1.1.40
3.2.8.1.1.1	3.1.1.41
3.2.8.1.1.1	3.1.1.44
3.2.8.1.1.11	3.1.1.40
3.2.8.1.1.12	3.1.1.40
3.2.8.1.1.13	3.1.1.40
3.2.8.1.1.14	3.1.1.40
3.2.8.1.1.15	3.1.1.39
3.2.8.1.1.2	3.1.1.39
3.2.8.1.2.1	3.1.1.44
3.2.8.1.2.10	3.1.1.46
3.2.8.1.2.11	3.1.1.39
3.2.8.1.2.12	3.1.1.39
3.2.8.1.2.13	3.1.4.10
3.2.8.1.2.14	3.1.4.10
3.2.8.1.2.15	3.1.1.46
3.2.8.1.2.16	3.1.1.46
3.2.8.1.2.17	3.1.1.46
3.2.8.1.2.18	3.1.4.10
3.2.8.1.2.19	3.1.1.46
3.2.8.1.2.2	3.1.1.44
3.2.8.1.2.20	3.1.1.46
3.2.8.1.2.3	3.1.1.44
3.2.8.1.2.4	3.1.1.15
3.2.8.1.2.5	3.1.1.15
3.2.8.1.2.5	3.1.4.9
3.2.8.1.2.6	3.1.1.15
3.2.8.1.2.7	3.1.2.17
3.2.8.1.2.8	3.1.1.46
3.2.8.1.2.9	3.1.4.10
3.2.8.1.3.1	3.1.1.42
3.2.8.1.3.2	3.1.3.9
3.2.8.1.3.3	3.1.1.15
3.2.8.1.3.4	3.1.1.15
3.2.8.1.3.4	3.1.4.9
3.2.8.1.3.5	3.1.1.15
3.2.8.1.3.6	3.1.1.42
3.2.8.1.3.6	3.1.2.18
3.2.8.1.3.7	3.1.1.42
3.2.8.1.3.8	3.1.1.42
3.2.8.1.3.9	3.1.1.42
3.2.8.1.3.10	3.1.1.39
3.2.8.1.3.11	3.1.1.39
3.2.8.1.3.12	3.1.1.42
3.2.8.1.3.13	3.1.1.42
3.2.8.1.3.14	3.1.1.42
3.2.8.1.3.15	3.1.1.42
3.2.8.1.3.16	3.1.1.42
3.2.8.1.3.17	3.1.1.42
3.2.8.1.3.18	3.1.1.42
3.2.8.1.3.19	3.1.1.42
3.2.8.1.3.20	3.1.1.42
3.2.8.1.4.1	3.1.1.43
3.2.8.1.4.1	3.1.1.44
3.2.8.1.4.2	3.1.1.43
3.2.8.1.4.2	3.1.1.44
3.2.8.1.4.3	3.1.1.41
3.2.8.1.4.3	3.1.1.42
3.2.8.1.4.4	3.1.1.44
3.2.8.1.4.5	3.1.1.39
3.2.8.1.4.6	3.1.1.41
3.2.8.1.4.6	3.1.1.42
3.2.8.1.4.7	3.1.1.44
3.2.8.1.4.8	3.1.1.41
3.2.8.1.4.8	3.1.1.42
3.2.8.1.4.9	3.1.1.41
3.2.8.1.4.9	3.1.1.42
3.2.8.1.4.10	3.1.1.44
3.2.8.1.4.11	3.1.1.39
3.2.8.1.4.12	3.1.1.39
3.2.8.1.4.13	3.1.1.44
3.2.8.1.4.14	3.1.1.39
3.2.8.1.4.15	3.1.1.39
3.2.8.1.4.16	3.1.1.44
3.2.8.1.4.17	3.1.4.10
3.2.8.1.4.18	3.1.4.10
3.2.8.1.4.19	3.1.1.41
3.2.8.1.4.20	3.1.1.41
3.2.8.1.4.21	3.1.1.41
3.2.8.1.4.22	3.1.1.41
3.2.8.1.4.23	3.1.1.40
3.2.8.1.4.24	3.1.1.40
3.2.8.1.4.25	3.1.1.40
3.2.8.1.5.1	3.1.1.24
3.2.8.2.1	3.1.2.15
3.2.8.2.2	3.1.2.16
3.2.8.2.3	3.1.2.17
3.2.8.2.4	3.1.2.18
3.2.8.3.1.1	3.1.1.46
3.2.8.3.1.1	3.1.3.8
3.2.8.3.2.1	3.1.1.42
3.2.8.3.2.1	3.1.3.1
3.2.8.3.2.1	3.1.3.10
3.2.8.3.2.2	3.1.1.42
3.2.8.3.2.2	3.1.3.10
3.2.8.3.2.3	3.1.3.10
3.2.8.3.2.4	3.1.3.10
3.2.8.3.2.5	3.1.3.10
3.2.8.3.2.6	3.1.3.10
3.2.8.4.1	3.1.1.15
3.2.8.4.2	3.1.1.15
3.2.8.4.3	3.1.1.15
3.2.8.4.4	3.1.1.15
3.2.8.4.5	3.1.1.15
3.2.8.4.6	3.1.1.15

6.2 Requirements to Architecture Components

The relationships between objects or components of the architecture and requirements contained in this specification will be documented in this section. This section will evolve as the architecture matures.

The table below is a preliminary mapping between Subsystem Requirements to Architectural Functional Objects. This mapping will be completed and other mappings drawn as the architecture is completed.

Table 6-4. Subsystem Requirement to Architecture Object Traceability

Subsystem	Subsystem Req ID	Arch Object Mapping
Core2Core	3.2.1.1.1	
Core2Core	3.2.1.1.2	
Core2Core	3.2.1.1.3	
Core2Core	3.2.1.1.4	Coordinate Data Coverage Area with Other Cores, Data Coverage Query
Core2Core	3.2.1.1.5	Coordinate Data Coverage Area with Other Cores, Data Coverage Characteristics Response
Core2Core	3.2.1.1.6	
Core2Core	3.2.1.1.7	Make Time Available to All Subsystems
Core2Core	3.2.1.1.8	
Core2Core	3.2.1.1.9	
Core2Core	3.2.1.1.10	
Core2Core	3.2.1.1.11	Modify Operational State
Core2Core	3.2.1.1.12	Monitor Core Health and Safety
Core2Core	3.2.1.1.13	Monitor Core Health and Safety
Core2Core	3.2.1.1.14	Monitor Status of other Cores
Core2Core	3.2.1.1.15	
Core2Core	3.2.1.1.16	
Core2Core	3.2.1.1.17	
Core2Core	3.2.1.1.18	Monitor Status of other Cores
Core2Core	3.2.1.1.19	Monitor Status of other Cores
Core2Core	3.2.1.1.20	Maintain Core Operational Configuration
Core2Core	3.2.1.1.21	Maintain Core Operational Configuration
Core2Core	3.2.1.1.22	Maintain Core Operational Configuration, Provide Service Status to other Cores
Core2Core	3.2.1.1.23	Maintain Core Operational Configuration
Core2Core	3.2.1.1.24	Maintain Core Operational Configuration, Monitor Status of other Cores, Exchange Misbe havior Reports with other Cores
Core2Core	3.2.1.1.25	Maintain Core Operational Configuration, Exchange Misbe havior Reports with other Cores
Core2Core	3.2.1.1.25.1	Monitor Status of other Cores, Exchange Misbe havior Reports with other Cores
Core2Core	3.2.1.1.26	Maintain Core Operational Configuration
Core2Core	3.2.1.1.26.1	Monitor Status of other Cores

Subsystem	Subsystem Req ID	Arch Object Mapping
Core2Core	3.2.1.1.26.2	Monitor Status of other Cores
Core2Core	3.2.1.1.26.3	Monitor Status of other Cores
Core2Core	3.2.1.1.26.4	
Core2Core	3.2.1.1.27	
Core2Core	3.2.1.1.27.1	
Core2Core	3.2.1.1.27.2	
Core2Core	3.2.1.1.27.3	
Core2Core	3.2.1.1.27.4	
Core2Core	3.2.1.1.27.5	
Core2Core	3.2.1.1.27.6	
Core2Core	3.2.1.1.27.7	Coordinate Certificate Distribution with Other Cores
Core2Core	3.2.1.1.27.8	Coordinate Certificate Distribution with Other Cores
Core2Core	3.2.1.1.28	Maintain Core Operational Configuration
Core2Core	3.2.1.1.28.1	Maintain Core Operational Configuration
Core2Core	3.2.1.1.28.2	Maintain Core Operational Configuration
Core2Core	3.2.1.1.28.3	Maintain Core Operational Configuration
Core2Core	3.2.1.1.28.4	Maintain Core Operational Configuration
Core2Core	3.2.1.1.29	Maintain Core Operational Configuration
Core2Core	3.2.1.1.29.1	Maintain Core Operational Configuration
Core2Core	3.2.1.1.29.2	Maintain Core Operational Configuration
Core2Core	3.2.1.1.30	
Core2Core	3.2.1.1.31	Maintain Core Operational Configuration
Core2Core	3.2.1.1.32	Maintain Core Operational Configuration
Core2Core	3.2.1.1.33	Maintain Core Operational Configuration
Core2Core	3.2.1.2.1	
Core2Core	3.2.1.2.2	
Core2Core	3.2.1.3.1.1	
Core2Core	3.2.1.3.1.2	Provide Operator Interface to MM
Core2Core	3.2.1.3.1.3	
Core2Core	3.2.1.3.1.4	
Core2Core	3.2.1.3.2.1	
Core2Core	3.2.1.3.2.2	
Core2Core	3.2.1.3.2.3	
Core2Core	3.2.1.3.2.4	
Core2Core	3.2.1.3.2.5	
Core2Core	3.2.1.3.2.6	
Core2Core	3.2.1.4.1	
Core2Core	3.2.1.4.2	
Core2Core	3.2.1.4.3	
Core2Core	3.2.1.4.4	Data Coverage Characteristics
Data Distribution	3.2.2.1.1.1	Maintain System User Data Subscriptions, Modify Data Acceptance Catalogs
Data Distribution	3.2.2.1.1.2	Maintain System User Data Subscriptions, Modify Data Acceptance

Subsystem	Subsystem Req ID	Arch Object Mapping
		Catalogs
Data Distribution	3.2.2.1.1.3	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.1.4	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.1.5	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.1.6	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.1.7	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.1.8	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.2	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.3	Maintain System User Data Subscriptions, Modify Data Acceptance Catalogs
Data Distribution	3.2.2.1.3.1	Maintain System User Data Subscriptions, Modify Data Acceptance Catalogs
Data Distribution	3.2.2.1.3.2	Maintain System User Data Subscriptions, Modify Data Acceptance Catalogs
Data Distribution	3.2.2.1.4	Data Acceptance Query, Match Data to Data Subscribers
Data Distribution	3.2.2.1.5	Data Acceptance Query, Match Data to Data Subscribers
Data Distribution	3.2.2.1.6	
Data Distribution	3.2.2.1.7	Modify Operational State, Generic Application Component
Data Distribution	3.2.2.1.8.1	Distribute Direct Data Acceptance Information, Maintain Direct Data Acceptance Catalog, Data Acceptance Changes, Data Acceptance Query, Direct Data Distribution Info
Data Distribution	3.2.2.1.9.1	
Data Distribution	3.2.2.1.10	
Data Distribution	3.2.2.1.10.1	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.2	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.3	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.4	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.5	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.6	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.7	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.8	Maintain Data Acceptance Catalog
Data Distribution	3.2.2.1.10.9	Provide Data to Subscribing System Users, Repackage Data
Data Distribution	3.2.2.1.10.10	Provide Data to Subscribing System Users, Repackage Data
Data Distribution	3.2.2.1.11	Modify Operational State
Data Distribution	3.2.2.1.12	
Data Distribution	3.2.2.1.13	
Data Distribution	3.2.2.1.13.1	
Data Distribution	3.2.2.1.14	
Data Distribution	3.2.2.1.15	
Data Distribution	3.2.2.1.16	
Data Distribution	3.2.2.1.17	Identify Potentially Misbehaving Data Provider, Data
Data Distribution	3.2.2.1.18	Identify Potentially Misbehaving Data Provider, Data, Identify Misbehaving System Users
Data Distribution	3.2.2.1.19	Identify Potentially Misbehaving Data Provider, Data

Subsystem	Subsystem Req ID	Arch Object Mapping
Data Distribution	3.2.2.1.20.1	Provide Operator Interface to DD
Data Distribution	3.2.2.1.20.2	Provide Operator Interface to DD
Data Distribution	3.2.2.1.20.3	Provide Operator Interface to DD
Data Distribution	3.2.2.1.20.4	Provide Operator Interface to DD
Data Distribution	3.2.2.1.20.5	
Data Distribution	3.2.2.1.20.6	
Data Distribution	3.2.2.1.20.7	
Data Distribution	3.2.2.1.20.8	Provide Service Status to other Cores
Data Distribution	3.2.2.1.20.9	Provide Service Status to other Cores
Data Distribution	3.2.2.1.20.10	
Data Distribution	3.2.2.1.20.11.1	
Data Distribution	3.2.2.1.21.1	
Data Distribution	3.2.2.1.21.2	Modify Operational State
Data Distribution	3.2.2.1.21.3	
Data Distribution	3.2.2.1.21.4	
Data Distribution	3.2.2.1.21.5	
Data Distribution	3.2.2.1.21.6	
Data Distribution	3.2.2.1.21.7	Modify Operational State
Data Distribution	3.2.2.1.21.8	
Data Distribution	3.2.2.1.22.1	Make Time Available to All Subsystems
Data Distribution	3.2.2.2.1	
Data Distribution	3.2.2.3.1.1	
Data Distribution	3.2.2.3.1.2	
Data Distribution	3.2.2.3.1.3	
Data Distribution	3.2.2.3.2.1	
Data Distribution	3.2.2.3.2.2	
Data Distribution	3.2.2.3.2.3	
Data Distribution	3.2.2.3.2.4	
Data Distribution	3.2.2.3.2.5	
Data Distribution	3.2.2.3.2.6	
Data Distribution	3.2.2.4.1	Data Types and Sources
Data Distribution	3.2.2.4.2	Data Types and Sources
Data Distribution	3.2.2.4.3	
Data Distribution	3.2.2.4.4	Data Type and Source Request
Data Distribution	3.2.2.4.5	Data Type and Source Request
Data Distribution	3.2.2.4.6	Data Types and Sources, Data Acceptance Changes, Data Acceptance or Discard, Data Type and Source, Permission, Data Type and Source Request, Existing Acceptance and/or Changes, Data Coverage Conflict, and Data Acceptance Details
Data Distribution	3.2.2.4.7	Data Type and Source Request, Existing Acceptance and/or Changes, Data Description, Subscription Details, Subscriber ID, Data Subscription Details, and Data Subscription Changes.
Misbehavior Management	3.2.3.1.1	

Subsystem	Subsystem Req ID	Arch Object Mapping
Misbehavior Management	3.2.3.1.2.1	Identify Potentially Misbehaving Data Provider, Manage Misbehavior Reports, Manually Confirm/Identify Misbehaving Users
Misbehavior Management	3.2.3.1.2.2	Provide Operator Interface to MM
Misbehavior Management	3.2.3.1.2.3	Provide Operator Interface to MM
Misbehavior Management	3.2.3.1.3.1	Identify Misbehaving Operators, Provide Operator Interface to MM
Misbehavior Management	3.2.3.1.3.2	Identify Misbehaving Operators
Misbehavior Management	3.2.3.1.3.3	Identify Misbehaving Operators, Receive Internal Misbehavior Reports
Misbehavior Management	3.2.3.1.3.4	Receive Internal Misbehavior Reports, Receive Internal Misbehavior Reports
Misbehavior Management	3.2.3.1.3.5	
Misbehavior Management	3.2.3.1.3.6	Receive System User Misbehavior Reports
Misbehavior Management	3.2.3.1.3.7	Receive System User Misbehavior Reports
Misbehavior Management	3.2.3.1.3.8	Modify Operational State
Misbehavior Management	3.2.3.1.4.1	
Misbehavior Management	3.2.3.1.4.2	Modify Operational State, Provide Operator Interface to MM
Misbehavior Management	3.2.3.1.4.3	
Misbehavior Management	3.2.3.1.4.4	
Misbehavior Management	3.2.3.1.4.5	
Misbehavior Management	3.2.3.1.4.6	
Misbehavior Management	3.2.3.1.4.7	
Misbehavior Management	3.2.3.1.5.1	Manage Misbehavior Reports
Misbehavior Management	3.2.3.1.5.2	Identify Misbehaving System Users, Manually Confirm/Identify Misbehaving Users
Misbehavior Management	3.2.3.1.5.2.1	
Misbehavior Management	3.2.3.1.5.2.2	
Misbehavior Management	3.2.3.1.5.3	
Misbehavior Management	3.2.3.1.5.4	Provide Operator Interface to MM
Misbehavior Management	3.2.3.1.5.5	Exchange Misbehavior Reports with other Cores
Misbehavior Management	3.2.3.1.6.1	Make Time Available to All Subsystems
Misbehavior Management	3.2.3.2.1	Identify Misbehaving System Users
Misbehavior Management	3.2.3.2.2	
Misbehavior Management	3.2.3.2.3	
Misbehavior Management	3.2.3.3.1.1	
Misbehavior Management	3.2.3.3.1.2	Exchange Misbehavior Reports with other Cores, Manage Misbehavior Reports
Misbehavior Management	3.2.3.3.1.3	
Misbehavior Management	3.2.3.3.2.1	
Misbehavior Management	3.2.3.3.2.2	
Misbehavior Management	3.2.3.3.2.3	
Misbehavior Management	3.2.3.3.2.4	
Misbehavior Management	3.2.3.4.1	Identify Misbehaving System Users
Misbehavior Management	3.2.3.4.2	Identify Misbehaving System Users
Misbehavior Management	3.2.3.4.3	

Subsystem	Subsystem Req ID	Arch Object Mapping
Misbehavior Management	3.2.3.4.4	
Misbehavior Management	3.2.3.4.5	
Misbehavior Management	3.2.3.4.6	
Network Services	3.2.4.1.1.1	
Network Services	3.2.4.1.1.2	Maintain Geo-cast Information, Intrusion Prevention
Network Services	3.2.4.1.1.3	Maintain Geo-cast Information, Geo-cast data request, Intrusion Prevention
Network Services	3.2.4.1.1.4	Maintain Geo-cast Information, Geo-cast data request, Intrusion Prevention
Network Services	3.2.4.1.1.5	Maintain Geo-cast Information
Network Services	3.2.4.1.1.6	Maintain Geo-cast Information
Network Services	3.2.4.1.1.7	
Network Services	3.2.4.1.1.8	Geo-cast data request
Network Services	3.2.4.1.1.9	Geo-cast facilitation information, Provide Geo-Cast Information to System User
Network Services	3.2.4.1.2.1	
Network Services	3.2.4.1.2.2	
Network Services	3.2.4.1.2.3	
Network Services	3.2.4.1.3.1	
Network Services	3.2.4.1.3.2	
Network Services	3.2.4.1.3.3	
Network Services	3.2.4.1.3.4	
Network Services	3.2.4.1.3.5	
Network Services	3.2.4.1.3.6	Modify Operational State
Network Services	3.2.4.1.3.7	
Network Services	3.2.4.1.3.8	
Network Services	3.2.4.1.3.9	
Network Services	3.2.4.1.3.10	
Network Services	3.2.4.1.3.11	Intrusion Detection
Network Services	3.2.4.1.3.12	Intrusion Detection
Network Services	3.2.4.1.3.13	
Network Services	3.2.4.1.3.14	
Network Services	3.2.4.1.4.1	Make Time Available to All Subsystems
Network Services	3.2.4.2.1	
Network Services	3.2.4.2.2	
Network Services	3.2.4.3.1.1	
Network Services	3.2.4.3.1.2	
Network Services	3.2.4.3.1.3	
Network Services	3.2.4.3.1.4	
Network Services	3.2.4.3.2.1	
Network Services	3.2.4.3.2.2	
Network Services	3.2.4.3.2.3	
Network Services	3.2.4.3.2.4	

Subsystem	Subsystem Req ID	Arch Object Mapping
Network Services	3.2.4.3.2.5	
Network Services	3.2.4.3.2.6	
Network Services	3.2.4.4.1	
Service Monitor	3.2.5.1.1	Monitor Core Services Performance
Service Monitor	3.2.5.1.1.1	Monitor Core Services Performance
Service Monitor	3.2.5.1.1.2	
Service Monitor	3.2.5.1.1.3	
Service Monitor	3.2.5.1.1.4	Provide Operator Interface, Monitor Core Services Performance, Monitor Service Control Node Performance
Service Monitor	3.2.5.1.1.5	Provide Operator Interface, Monitor Core Services Performance
Service Monitor	3.2.5.1.1.6	Provide Operator Interface, Monitor Core Services Performance
Service Monitor	3.2.5.1.1.7	Log System State and Performance
Service Monitor	3.2.5.1.1.8	Monitor Core Services Performance, Monitor Core Health and Safety
Service Monitor	3.2.5.1.1.9	Monitor Core Services Performance, Monitor Core Health and Safety
Service Monitor	3.2.5.1.1.10	Monitor Core Services Performance, Monitor Core Health and Safety
Service Monitor	3.2.5.1.1.11	Monitor Core Services Performance
Service Monitor	3.2.5.1.1.12	Monitor Core Services Performance
Service Monitor	3.2.5.1.1.13	Monitor Core Services Performance
Service Monitor	3.2.5.1.1.14	Provide Operator Interface
Service Monitor	3.2.5.1.1.15	Provide Operator Interface, Modify Operational State
Service Monitor	3.2.5.1.1.16	Provide Operator Interface
Service Monitor	3.2.5.1.1.17	Monitor Core Services Performance, Monitor Core Health and Safety
Service Monitor	3.2.5.1.1.18	Provide Operator Interface, Monitor Core Services Performance
Service Monitor	3.2.5.1.2	
Service Monitor	3.2.5.1.3	
Service Monitor	3.2.5.1.4	
Service Monitor	3.2.5.1.5	
Service Monitor	3.2.5.1.6	
Service Monitor	3.2.5.1.7	
Service Monitor	3.2.5.1.8	Provide Operator Interface
Service Monitor	3.2.5.1.8.1	Provide Operator Interface
Service Monitor	3.2.5.1.9	
Service Monitor	3.2.5.1.10	
Service Monitor	3.2.5.1.11	Monitor Core Health and Safety
Service Monitor	3.2.5.1.11.1	Provide Operator Interface, Monitor Core Services Performance
Service Monitor	3.2.5.1.11.2	
Service Monitor	3.2.5.1.11.3	
Service Monitor	3.2.5.1.11.4	
Service Monitor	3.2.5.1.11.5	Provide Operator Interface, Monitor Core Health and Safety
Service Monitor	3.2.5.1.11.6	Provide Operator Interface, Monitor Core Health and Safety
Service Monitor	3.2.5.1.11.7	Provide Operator Interface
Service Monitor	3.2.5.1.11.8	Provide Operator Interface
Service Monitor	3.2.5.1.11.9	Monitor Core Health and Safety

Subsystem	Subsystem Req ID	Arch Object Mapping
Service Monitor	3.2.5.1.11.10	Log System State and Performance
Service Monitor	3.2.5.1.11.11	Provide Operator Interface
Service Monitor	3.2.5.1.11.12	Log System State and Performance, Monitor Core Health and Safety
Service Monitor	3.2.5.1.12	Provide Operator Interface
Service Monitor	3.2.5.1.12.1	Provide Operator Interface
Service Monitor	3.2.5.1.12.2	Provide Operator Interface
Service Monitor	3.2.5.1.12.3	Provide Operator Interface
Service Monitor	3.2.5.1.12.4	Provide Operator Interface
Service Monitor	3.2.5.1.12.5	Provide Operator Interface
Service Monitor	3.2.5.1.13	
Service Monitor	3.2.5.1.14	Provide Operator Interface, Modify Operational State
Service Monitor	3.2.5.1.15	
Service Monitor	3.2.5.1.16	
Service Monitor	3.2.5.1.17	
Service Monitor	3.2.5.1.18	
Service Monitor	3.2.5.1.19	Provide Operator Interface
Service Monitor	3.2.5.1.20	
Service Monitor	3.2.5.1.21	Provide Operator Interface
Service Monitor	3.2.5.1.22	Make Time Available to All Subsystems
Service Monitor	3.2.5.2.1	Provide Operator Interface
Service Monitor	3.2.5.2.2	Provide Operator Interface
Service Monitor	3.2.5.2.3	Provide Operator Interface
Service Monitor	3.2.5.2.4	
Service Monitor	3.2.5.2.5	Monitor Core Physical Security, Take Action in Response to Physical Environmental Issue
Service Monitor	3.2.5.3.1.1	
Service Monitor	3.2.5.3.2.1	
Service Monitor	3.2.5.3.1.2	
Service Monitor	3.2.5.3.1.3	Provide Operator Interface
Service Monitor	3.2.5.4.2	
Service Monitor	3.2.5.4.3	
Service Monitor	3.2.5.4.4	
Service Monitor	3.2.5.4.5	
Service Monitor	3.2.5.4.6	
Time	3.2.6.1.1	Get Time from External Available Source
Time	3.2.6.1.2	Make Time Available to All Subsystems
Time	3.2.6.1.3	
Time	3.2.6.1.4	
Time	3.2.6.1.5	Get Time from External Available Source
Time	3.2.6.1.6	
Time	3.2.6.1.7	
Time	3.2.6.1.8	
Time	3.2.6.1.9	

Subsystem	Subsystem Req ID	Arch Object Mapping
Time	3.2.6.1.10	Modify Operational State
Time	3.2.6.1.11	
Time	3.2.6.1.12	Modify Operational State
Time	3.2.6.2.1	
Time	3.2.6.2.2	Get Time from External Available Source
Time	3.2.6.3.1.1	Get Time from External Available Source
Time	3.2.6.3.1.2	Make Time Available to All Subsystems
Time	3.2.6.3.2.1	
Time	3.2.6.3.2.2	
Time	3.2.6.3.2.3	
Time	3.2.6.3.2.4	
Time	3.2.6.3.2.5	
Time	3.2.6.3.2.6	
Time	3.2.6.3.2.7	
User Permissions	3.2.7.1.1.1	Check User Permission
User Permissions	3.2.7.1.1.2	Check User Permission
User Permissions	3.2.7.1.1.3	Check User Permission
User Permissions	3.2.7.1.1.4	Check User Permission
User Permissions	3.2.7.1.2.1	
User Permissions	3.2.7.1.2.2	
User Permissions	3.2.7.1.2.3	
User Permissions	3.2.7.1.2.4	
User Permissions	3.2.7.1.2.5	
User Permissions	3.2.7.1.2.6	
User Permissions	3.2.7.1.2.7	Identify Misbehaving Operators
User Permissions	3.2.7.1.2.8	Identify Misbehaving Operators
User Permissions	3.2.7.1.2.9	Identify Misbehaving System Users, Manually Confirm/Identify Misbehaving Users, Receive Internal Misbehavior Reports
User Permissions	3.2.7.1.2.10	
User Permissions	3.2.7.1.2.11	
User Permissions	3.2.7.1.2.12	
User Permissions	3.2.7.1.2.13	
User Permissions	3.2.7.1.2.14	Modify Operational State
User Permissions	3.2.7.1.3.1	Make Time Available to All Subsystems
User Permissions	3.2.7.2.1	
User Permissions	3.2.7.2.2	
User Permissions	3.2.7.2.3	
User Permissions	3.2.7.2.4	
User Permissions	3.2.7.3.1.1	
User Permissions	3.2.7.3.1.1.1	Revoke Operator Permissions, Revoke User Permissions
User Permissions	3.2.7.3.1.1.2	
User Permissions	3.2.7.3.1.1.3	
User Permissions	3.2.7.3.1.1.4	

Subsystem	Subsystem Req ID	Arch Object Mapping
User Permissions	3.2.7.3.1.2	
User Permissions	3.2.7.3.1.2.1	
User Permissions	3.2.7.3.1.2.2	
User Permissions	3.2.7.3.1.2.3	
User Permissions	3.2.7.3.1.2.4	
User Permissions	3.2.7.3.1.2.5	
User Permissions	3.2.7.3.1.2.6	
User Permissions	3.2.7.3.1.2.7	
User Permissions	3.2.7.3.1.2.8	
User Permissions	3.2.7.3.1.3	
User Permissions	3.2.7.3.1.3.1	
User Permissions	3.2.7.3.1.3.2	
User Permissions	3.2.7.3.1.3.3	
User Permissions	3.2.7.3.1.3.4	
User Permissions	3.2.7.3.1.3.5	
User Permissions	3.2.7.3.1.3.6	
User Permissions	3.2.7.3.1.3.7	
User Permissions	3.2.7.3.1.3.8	
User Permissions	3.2.7.3.1.3.9	
User Permissions	3.2.7.3.1.4	
User Permissions	3.2.7.3.1.4.1	
User Permissions	3.2.7.3.1.4.2	
User Permissions	3.2.7.3.1.4.3	
User Permissions	3.2.7.3.1.4.4	
User Permissions	3.2.7.3.2.1	
User Permissions	3.2.7.3.2.2	
User Permissions	3.2.7.3.2.3	
User Permissions	3.2.7.3.2.4	
User Permissions	3.2.7.3.2.5	
User Permissions	3.2.7.3.2.6	
User Permissions	3.2.7.4.1	User ID, Subscribing ID, Permission, Operator ID
User Permissions	3.2.7.4.2	User ID, Subscribing ID, Permission, Operator ID
User Permissions	3.2.7.4.3	User ID, Subscribing ID, Permission
User Permissions	3.2.7.4.4	User ID, Subscribing ID, Permission
User Permissions	3.2.7.4.5	User ID, Subscribing ID, Permission
User Permissions	3.2.7.4.6	User ID, Subscribing ID, Permission
User Permissions	3.2.7.4.7	Provider ID
User Security	3.2.8.1.1.3	Decrypt Messages Received Encrypted
User Security	3.2.8.1.1.10	
User Security	3.2.8.1.1.4	Decrypt Messages Received Encrypted
User Security	3.2.8.1.1.5	Verify Signature of Received Messages
User Security	3.2.8.1.1.6	Encrypt Messages

Subsystem	Subsystem Req ID	Arch Object Mapping
User Security	3.2.8.1.1.7	Sign Messages
User Security	3.2.8.1.1.8	Encrypt Messages
User Security	3.2.8.1.1.9	Sign Messages
User Security	3.2.8.1.1.1	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.1.11	Sign Messages
User Security	3.2.8.1.1.12	
User Security	3.2.8.1.1.13	
User Security	3.2.8.1.1.14	
User Security	3.2.8.1.1.15	Identify Potentially Misbehaving Data Provider, Misbehavior report, Identify Misbehaving System Users, Manually Confirm/Identify Misbehaving Users
User Security	3.2.8.1.1.2	Verify Signature of Received Messages
User Security	3.2.8.1.2.1	
User Security	3.2.8.1.2.10	
User Security	3.2.8.1.2.11	Verify Signature of Received Messages
User Security	3.2.8.1.2.12	
User Security	3.2.8.1.2.13	
User Security	3.2.8.1.2.14	
User Security	3.2.8.1.2.15	
User Security	3.2.8.1.2.16	
User Security	3.2.8.1.2.17	Exchange CRLs with other Cores
User Security	3.2.8.1.2.18	Exchange CRLs with other Cores
User Security	3.2.8.1.2.19	Exchange CRLs with other Cores
User Security	3.2.8.1.2.2	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.2.20	Exchange CRLs with other Cores
User Security	3.2.8.1.2.3	Provide DSRC Identity Certificates
User Security	3.2.8.1.2.4	
User Security	3.2.8.1.2.5	
User Security	3.2.8.1.2.6	
User Security	3.2.8.1.2.7	
User Security	3.2.8.1.2.8	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.2.9	Exchange CRLs with other Cores
User Security	3.2.8.1.3.1	Maintain Core X.509 Certificate
User Security	3.2.8.1.3.2	Provide X.509 Identity Certificates
User Security	3.2.8.1.3.3	
User Security	3.2.8.1.3.4	
User Security	3.2.8.1.3.5	Maintain Core X.509 Certificate
User Security	3.2.8.1.3.6	Manage X.509 CRL
User Security	3.2.8.1.3.7	Provide X.509 Identity Certificates
User Security	3.2.8.1.3.8	Exchange CRLs with other Cores
User Security	3.2.8.1.3.9	
User Security	3.2.8.1.3.10	Verify Signature of Received Messages
User Security	3.2.8.1.3.11	

Subsystem	Subsystem Req ID	Arch Object Mapping
User Security	3.2.8.1.3.12	
User Security	3.2.8.1.3.13	
User Security	3.2.8.1.3.14	
User Security	3.2.8.1.3.15	Provide X.509 Identity Certificates
User Security	3.2.8.1.3.16	Exchange CRLs with other Cores
User Security	3.2.8.1.3.17	Exchange CRLs with other Cores
User Security	3.2.8.1.3.18	Exchange CRLs with other Cores
User Security	3.2.8.1.3.19	Exchange CRLs with other Cores
User Security	3.2.8.1.3.20	
User Security	3.2.8.1.4.1	
User Security	3.2.8.1.4.2	
User Security	3.2.8.1.4.3	
User Security	3.2.8.1.4.4	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.4.5	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.4.6	
User Security	3.2.8.1.4.7	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.4.8	
User Security	3.2.8.1.4.9	
User Security	3.2.8.1.4.10	Provide DSRC Anonymous Certificates
User Security	3.2.8.1.4.11	Verify Signature of Received Messages, Provide DSRC Identity Certificates
User Security	3.2.8.1.4.12	
User Security	3.2.8.1.4.13	Provide DSRC Identity Certificates
User Security	3.2.8.1.4.14	Verify Signature of Received Messages, Provide DSRC Identity Certificates
User Security	3.2.8.1.4.15	
User Security	3.2.8.1.4.16	
User Security	3.2.8.1.4.17	
User Security	3.2.8.1.4.18	
User Security	3.2.8.1.4.19	Exchange CRLs with other Cores
User Security	3.2.8.1.4.20	Exchange CRLs with other Cores
User Security	3.2.8.1.4.21	Exchange CRLs with other Cores
User Security	3.2.8.1.4.22	Exchange CRLs with other Cores
User Security	3.2.8.1.4.23	
User Security	3.2.8.1.4.24	
User Security	3.2.8.1.4.25	
User Security	3.2.8.1.5.1	Make Time Available to All Subsystems
User Security	3.2.8.2.1	
User Security	3.2.8.2.2	
User Security	3.2.8.2.3	
User Security	3.2.8.2.4	Manage X.509 CRL
User Security	3.2.8.3.1.1	
User Security	3.2.8.3.1.2	

Subsystem	Subsystem Req ID	Arch Object Mapping
User Security	3.2.8.3.1.3	
User Security	3.2.8.3.2.1	
User Security	3.2.8.3.2.2	
User Security	3.2.8.3.2.3	
User Security	3.2.8.3.2.4	
User Security	3.2.8.3.2.5	
User Security	3.2.8.3.2.6	
User Security	3.2.8.4.1	Maintain DSRC Anonymous Certificates
User Security	3.2.8.4.2	Maintain DSRC Identity Certificates
User Security	3.2.8.4.3	
User Security	3.2.8.4.4	
User Security	3.2.8.4.5	Manage X.509 CRL
User Security	3.2.8.4.6	

7 Terminology

This section includes definition of key terms and a list of Abbreviations and Acronyms used in this document.

7.1 Glossary

Table 7-1. Glossary

Term	Definition
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Analysis	The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other.
Anonymity	Lacking individuality, distinction, and recognizability within message exchanges.
Anonymous Certificates	Is a certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the *connected vehicle* program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
Application	A computer software program with an interface, enabling people to use the computer as a tool to accomplish a specific task.
Application User	One who interfaces with Application Layer-based software for a function or feature.
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.
Authorization	The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

Term	Definition
Assumption	A judgment about unknown factors and the future which is made in analyzing alternative courses of action.
Back Office	See Center
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.
Boundaries	The area of management and control for a Core System. It could be by latitude/longitude or by county or by regional jurisdictions.
Catalog	Used by the Data Distribution Subsystem as a repository for maintaining data publishers information including the type of data they are transmitting, frequency of that data, address, data source, etc.
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of the Core System ConOps these are considered the same.
Class of Service (CoS)	Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.
Compatibility issues	Conflict with two Core Systems, such as different Core System software versions that aren't compatible.
Concept of Operations (ConOps)	A user-oriented document that describes a system's operational characteristics from the end user's viewpoint.
Configure/configuration	The choose option(s) in order to create a custom system.
Constraint	An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.
Contract	In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project.

Term	Definition
Control	To exercise influence over.
Coordinate coverage	When two Core System boundaries are near or overlapping, there needs to be an agreement between the two Core Systems who should be the one to provide coverage.
Core System Personnel-controlled rules	The conditions to identify misbehavior activity, including the need to revoke credentials from such reported misbehaving users.
Core System Personnel	This represents the staff that operates and maintains the Core System. In addition to network managers and operations personnel, Core System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployers and Testers.
Core System User	See System User.
Correlation processing	To process data for misbehavior pattern matching and to look for signatures of known misbehavior users.
Data Consumer	A user or system that is receiving or using data from another user or system.
Data Provider	A user or System User that is supplying or transmitting data to another user or system.
Data Provisioning	The act of a System User providing data to a consumer.
Degraded Mode	In the degraded mode, the subsystem is impaired to a significant extent: its ability to provide services is greatly reduced or eliminated completely. Also, Service Monitor's ability to manage the subsystem may be impaired.
Degraded/Restricted Mode	If during the course of operating in a restricted mode there is a loss of functionality, or if while in degraded mode there is a need to enter restricted mode, the subsystem may enter the degraded/restricted mode. This mode is a combination of the restricted and degraded modes, where subsystem services are offered only to particular users, but performance is degraded.
Delta updates	Only the data that is new since the last block of data that was downloaded.
Denial of Service (DoS) attack	An explicit attempt by an attacker to prevent legitimate users of that system from accessing information or services. Examples include flooding the network with useless messages or attempting an overflow condition.
Deployability	Able to be deployed in existing roadway environments, without requiring replacement of existing systems in order to provide measurable improvements.

Term	Definition
Deployers	These users represent the initial installers for a Core System. Their interaction with the Core System itself will be similar to an administrator or maintainer in that they will be accessing system configuration files, setting parameters and policies as part of the initial installation and check out of the system before turning it over to the other Core System Personnel for regular operations.
Desirable features	Features that should be provided by the Core System.
Developers	These users are the actual software developers that build software enhancements for the system. They will be accessing the published interface definitions and configuration data about the Core System in order to develop additional features or expanded capabilities
Digital Certificate or Signature	A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute - www.sans.org website.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it.
Essential features	Features that shall be provided by the Core System.
Extensibility	The ability to add or modify functionality or features with little or no design changes.
External source-to-point	When the data provider communicates data directly to data consumers. No data is sent through the Core System, however, the Core System is involved with checking user permissions and maintains provider addresses to consumers as part of its data catalog.
Facility	A building or group of buildings housing a Core System with access restrictions.

Term	Definition
Faculty backup services	When failed services of a Core System has been backed up by another Core System that has those same services available.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSE and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Flexibility	The ability to adjust or adapt to external changes with little or no design changes.
Functionality	The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product.
Geocast	The delivery of a message to a group of network destinations identified by their geographic locations.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Health of the Core System	The overall Core System's operational condition. This includes not only errors and alerts from the system; but intermittent errors and slow performance conditions that may not currently degrade the system, but is not necessarily a healthy system. Intermittent and slow performance conditions can be mitigated before it does degrade the system.
Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Installation State	This state includes all pre-operational activities necessary to plan, develop, install and verify the procedures and system configurations used to support the Core System.
Integrity	To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible.

Term	Definition
Issuance	a) For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). b) For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Local Cache	Reserved areas of computer memory that are used to speed up instruction execution, data retrieval and data updating.
Maintainability	To keep in an existing operational state preserved from failure or decline of services (with minimum repair, efficiency, or validity).
Maintenance State	The administrator commands this state for a particular subsystem or to the whole Core System to replace an impaired component or to upgrade a component(s). Depending on the nature of maintenance planned, the impact on the Core System's ability to provide services may be impacted. Also, its ability to manage itself and provide visibility into how it is performing may be impacted.
Maintainers	These users interact with the system to install updated software; repair or upgrade hardware components to keep the system up to date and running efficiently.
Misbehaving user	A user who abuses, violates or resembles suspicions behavior to include wrong message types or frequencies, invalid logins and unauthorized access, etc; either purposeful or unintended.

Term	Definition
Mobile	These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information
Modes	Modes are typically phases within a State, which can occur automatically due to certain conditions. Such as, when in Operational State, there is an automatic transition to Degraded Mode because of a detected hardware failure. Modes are Normal, Degraded, Restricted and Degraded/Restricted.
Modifiable parameter	Non-static data that can be adjustable and updated when needed.
NIST Time	National Institute of Science and Technology (NIST) is the standard for Internet time using the Year, Month, Day, Hour, Minute, Second format. NIST adjusts and compensates for time zones and Daylight Savings Time.
Node	A Node is a physical hardware Engineering Object that is a run-time computational resource and generally has at least memory and processing capability. Run-time software Engineering Objects reside on nodes. A Node has some well-understood, possibly rapidly moving, location. A Node may be composed of two or more (sub) Nodes.
Normal Mode	In the normal mode, there is little or no functional or performance impacts on the ability of the subsystem to provide its services. In addition, the Service Monitor provides good visibility into how the subsystem is performing.
Open Standard	Is a standard that is publicly available and has various rights to use associated with it, and may also have various properties of how it was designed (e.g. open process). Open Standards may not mean open source. A true open source is typically free to both acquire and implement.
Operational State	This state includes all activities during the normal conduct of operations. This state also needs to be able to handle support for services from other Cores including fail-over and/or degraded services.
Optional features	Features that might be provided by the Core System.
On-Board Equipment (OBE)	Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.

Term	Definition
Operators	These are the day-to-day users of the Core System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.
Persistent connection	A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received.
Point of Service	The Core System which provides a "gatekeeping arrangement" to connected System Users with functions and capabilities.
Port	A Port is the physical element of a Node where a Link is connected. Nodes may have one or more Ports. Each Port may connect to one or more physical Ports on (sub) Nodes that are contained within the Node.
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively.
Problem domain	A set of similar problems that occur in an environment and lend themselves to common solutions.
Process	A series of actions, changes, or functions bringing about a result.
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).
Registration characteristics	Attributes of the System User's enrollment process into the Core System. This would include the System User's role(s) and permission(s) that have been granted by the Core System.
Registry	A data repository for the Core System publishers data types (with characteristics) allowed for the Publisher/Subscriber model, the data that is currently available by publishers and the data it currently has subscribers to.
Reliability	Providing consistent and dependable system output or results.
Request for Quotation (RFQ)	A request for services, research, or a product prepared by a customer and delivered to a contractor with the expectation that the contractor will respond with their proposed cost, schedule, and development approach.

Term	Definition
Restricted mode	In the restricted mode, the subsystem is capable of performing as expected; however certain services or features are disabled to support a specific event such as an evacuation. The restriction is determined by operators/entities outside of the system and subsequently implemented by the system in response to an authorized operation (command) from the external entity. This may also be implemented via a policy-based management system whereby policies (as specified by an authorized external entity) are automatically implemented by the Core System in response to detection of events, behaviors or performance thresholds. In a restricted mode, the Core System could curtail the use of particular subsystems to privileged users, such first responders and other emergency personnel.
Scalability	The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign.
Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Service	A set of related functionalities accessed using a prescribed interface.
Software	Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software.
States or Modes	A state is typically commanded or placed in that state by an operator; such as Installation, Operational, Maintenance, Training, and Standby States. Also a state is distinct system setting in which the same user input will produce different results than it would in other settings. Note: MIL STD 961E uses States and Modes interchangeably.
Subsystem	An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
Standby	The Core System or subsystem operating in a Standby state will be providing backup to one or more other Cores or other Core subsystems. From the standby state the Core or subsystem may take over the functions of another Core or subsystem if required. When operating in Standby state, the Core or subsystem should be continually evaluated on its ability to switch-in and take provide services for the Core or subsystem it is supporting.
Status	A quality which reflects various levels of normal, warning, severe, or failed conditions.

Term	Definition
System	(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment. (B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
System Need	A capability that is identified and supported within the Core System to accomplish a specific goal or solve a problem
System User	System Users refers to Mobile, Field, Center and other Core Systems.
Testers	These users verify the Core System's operation when any changes are made to its operating hardware or software.
Time	A measurable period during which an action, process or condition occurs.
Time-of-Day	Current hours, minutes and seconds within a day.
Time synchronization	Calibration adjustment of date, hour, minutes and seconds for keeping the same time within a system.
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Training	The administrator commands this state when it is used for imparting training on the Core features. Certain features like real-time display of log messages and debug messages may be enabled in the Training state which may not otherwise be accessible under normal conditions.
Transition	A passage from one state, stage, subject, or place to another
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.

Term	Definition
Unicast	The sending of a message to a single network destination identified by a unique address.
User	An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions.
User Classes	A category of user, typically with different user profiles and access rights to the system.
User Need	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.

7.2 Abbreviations and Acronyms

This section contains an alphabetical listing of abbreviations and acronyms used in this document.

Table 7-2. Abbreviation and Acronym List

Abbreviation or Acronym	Definition
AMS	Analysis, Modeling, and Simulation
AASHTO	American Association of State Highway and Transportation Officials
AMDS	Advisory Message Distribution Service
APTA	American Public Transportation Association
ASOS	Automated Surface Observing System
AWOS	Automated Weather Observing System
BAH	Booz Allen Hamilton
CA	Certification Authority
CALM	Communications Access for Land Mobile Standards
CAMP	Crash Avoidance Metrics Partnership
CCH	Control Channel (interval)
CCTV	Closed Circuit Television
CICAS	Cooperative Intersection Collision Avoidance Systems
CMP	Certificate Management Protocol
COM eSafety	Communications for eSafety
ConOps	Concept of Operations
COOPERS	Cooperative Systems for Intelligent Road Safety
COTS	Commercial off-the-shelf
CRL	Certification Revocation Lists
CVIS	Cooperative Vehicle Infrastructure System
CVO	Commercial Vehicles Operation
DCM	Data Capture Management
DGPS	Differential GPS
DMA	Dynamic Mobility Applications
DMS	Dynamic Message Signs
DNS	Domain Name System

Abbreviation or Acronym	Definition
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
EC	European Commission
EEBL	Emergency Electronic Break Light
ENOC	Enterprise Network Operations Center
ETSI	European Telecommunications Standards Institute
INCOSE	International Council on Systems Engineering
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FRAME	Framework Architecture Made for Europe
FTA	Federal Transit Administration
GADS	Green Action Decider System
GCS	Geocasting Service
GHz	Gigahertz
GIS	Geographical Information Systems
GPS	Global Positioning System
HIA	“Here I am” basic safety message
HOV	High Occupancy Vehicle
HRI	Highway Rail Intersection
ICM	Integrated Corridor Management
ID	Identifier or Identification
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INCOSE	International Council of Systems Engineers
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Standards Office
ISP	Internet Service Provider or Information Service Provider
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems

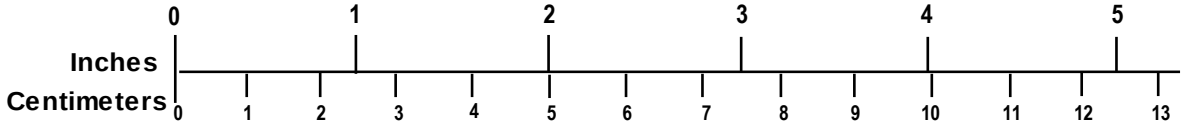
Abbreviation or Acronym	Definition
ITU	International Telecommunications Union
IVBSS	Integrated Vehicle-Based Safety Systems
JPO	Joint Program Office
LTE	Long Term Evolution
Mbps	Megabits per second
MIB	Management Information Base
NAVTEQ	Navigational Technology and Data Used to Develop Maps
NCAR	National Center for Atmospheric Research
NEMA	National Electrical Manufacturer's Association
NIST	National Institute of Standards and Technology
NSR	National System Requirements
NTCIP	National Transportation Communication for ITS Protocol
OBE	Onboard Equipment
OBU	On Board Unit
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
PDS	Probe Data Service
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure based on X.509 certificates
PII	Personally Identifiable Information
POC	Proof of Concept
PMP	Project Management Plan
PMU	Private Mobile User
PSMU	Public Service Mobile User
QC	Quality Control
RA	Registration Authority
RFC	Request for Comments
RITA	Research and Innovative Technology Administration's
RSE	Roadside Equipment
RSU	Roadside Unit
SAE	Society of Automobile Engineers

Abbreviation or Acronym	Definition
SCH	Service Channel (interval)
SDN	Service Delivery Node
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SPAT	Signal Phase and Timing
SRS	Software Requirements Specification
stm	State Machine
SUV	Sport Utility Vehicle
SyRS	System Requirements Specification
TBD	To Be Determined
TC	Technical Committee
TMC	Transportation Management Center
TRSP	Traffic Responsive (Signal Control)
US	United States
USDOT	US Department of Transportation
USNO	US Naval Observatory
VDT	Vehicle Data Translator
VII	Vehicle Infrastructure Integration
VIIC	Vehicle Infrastructure Integration Consortium
VMS	Variable Message Signal
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WAVE	Wireless Access in Vehicle Environment
WiMAX	Worldwide Interoperability for Microwave Access

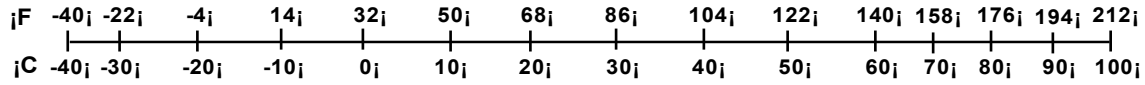
8 Metric/English Conversion Factors

ENGLISH TO METRIC	METRIC TO ENGLISH
LENGTH (APPROXIMATE)	**LENGTH (APPROXIMATE)**
1 inch (in) = 2.5 centimeters (cm)	1 millimeter (mm) = 0.04 inch (in)
1 foot (ft) = 30 centimeters (cm)	1 centimeter (cm) = 0.4 inch (in)
1 yard (yd) = 0.9 meter (m)	1 meter (m) = 3.3 feet (ft)
1 mile (mi) = 1.6 kilometers (km)	1 meter (m) = 1.1 yards (yd)
	1 kilometer (km) = 0.6 mile (mi)
AREA (APPROXIMATE)	**AREA (APPROXIMATE)**
1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)	1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m^2)	1 square meter (m^2) = 1.2 square yards (sq yd, yd^2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)	1 square kilometer (km^2) = 0.4 square mile (sq mi, mi^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)	10,000 square meters (m^2) = 1 hectare (ha) = 2.5 acres
1 acre = 0.4 hectare (he) = 4,000 square meters (m^2)	
MASS - WEIGHT (APPROXIMATE)	**MASS - WEIGHT (APPROXIMATE)**
1 ounce (oz) = 28 grams (gm)	1 gram (gm) = 0.036 ounce (oz)
1 pound (lb) = 0.45 kilogram (kg)	1 kilogram (kg) = 2.2 pounds (lb)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)	1 tonne (t) = 1,000 kilograms (kg) = 1.1 short tons
VOLUME (APPROXIMATE)	**VOLUME (APPROXIMATE)**
1 teaspoon (tsp) = 5 milliliters (ml)	1 milliliter (ml) = 0.03 fluid ounce (fl oz)
1 tablespoon (tbsp) = 15 milliliters (ml)	1 liter (l) = 2.1 pints (pt)
1 fluid ounce (fl oz) = 30 milliliters (ml)	1 liter (l) = 1.06 quarts (qt)
1 cup (c) = 0.24 liter (l)	1 liter (l) = 0.26 gallon (gal)
1 pint (pt) = 0.47 liter (l)	
1 quart (qt) = 0.96 liter (l)	
1 gallon (gal) = 3.8 liters (l)	
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)	1 cubic meter (m^3) = 36 cubic feet (cu ft, ft^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)	1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)
TEMPERATURE (EXACT)	**TEMPERATURE (EXACT)**
[(x-32)(5/9)] °F = y °C	[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSION



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50 SD Catalog No. C13 10286