



## ***NASA's Communications Provider***

---

---

# **National Aeronautics and Space Administration (NASA) Communications Service Office (CSO) Services Document (CSD)**

**July 2015**



## Preface

The National Aeronautics and Space Administration (NASA) Communications Service Office (CSO) Services Document (CSD) is prepared to aid CSO Customers with requesting available communications and network services as described in this document. Comments or questions pertaining to this document should be forwarded to the E-Mail address appearing in Appendix C, paragraph C.3.

This original document reflects service offerings delivered under the NASA Integrated Communications Services (NICS) contract, awarded in June, 2011. This information technology services contract enables the Information Technology (IT) Infrastructure Integration Program (I<sup>3</sup>P) vision for a seamless end-to-end Agency-wide communications infrastructure.

This document is under the Configuration Management (CM) of the Communications Services Office (CSO). Proposed changes to this document shall be submitted to the CSO along with supportive material justifying the proposed change before incorporation into the document.

## **Abstract**

This document provides information for requesting communications services available through the CSO organization. The CSO organization is an entity of the Office of the Chief Information Officer (OCIO). This document provides service descriptions, service operations, performance and maintenance for CSO services. It describes the funding methodology used for billing CSO Customers and key points of contact.

# Contents

<b>Revision History .....</b>	<b>ii</b>
<b>Preface.....</b>	<b>iii</b>
<b>Abstract.....</b>	<b>iv</b>
<b>1. Introduction .....</b>	<b>12</b>
1.1 Purpose.....	12
1.2 Scope.....	12
1.3 Document Organization .....	12
1.4 Related Documents .....	13
1.4.1 Applicable Documents .....	13
1.5 CSO Organization and Functions .....	14
1.6 Standard Practices .....	15
1.6.1 General .....	15
1.6.2 Guidelines .....	15
1.6.3 Acceptable Use Policy .....	16
1.6.4 Security .....	17
1.6.5 CSO Support Applications.....	18
1.7 Services.....	18
1.7.1 Planning for Products and Services .....	19
1.7.2 Service Implementation Test and Acceptance .....	19
1.7.3 CSO Value-Added Services.....	20
<b>2. Corporate Network Services .....</b>	<b>21</b>
2.1 Video Teleconferencing Services (ViTS).....	21
2.1.1 Service Description .....	21
2.1.2 ViTS Interface Types .....	22
2.1.3 ViTS Facilities .....	22
2.1.4 CSO Core Conference Rooms .....	22
2.1.5 Custom Conference Rooms .....	23
2.1.6 Multimedia Systems.....	23
2.1.7 High Definition ViTS Roll-About (VRA) Systems.....	23
2.1.8 Operations .....	24
2.1.9 Service Performance .....	24
2.1.10 Service Maintenance .....	25

2.2	DeskTop Mobile ViTS (DMV).....	25
2.2.1	Service Description .....	25
2.2.2	Operations .....	25
2.2.3	DMV Incident Reporting .....	26
2.2.4	Service Performance .....	26
2.2.5	Service Maintenance .....	26
2.3	Voice Teleconferencing System (VoTS) .....	26
2.3.1	Service Description .....	26
2.3.2	Premier .....	27
2.3.3	Standard.....	27
2.3.4	Instant Meeting.....	27
2.4	Voice Teleconferencing System (VoTS) Facilities .....	28
2.4.1	Operations .....	28
2.4.2	VoTS Incident Reporting.....	28
2.4.3	Service Performance .....	28
2.4.4	Service Maintenance .....	28
2.5	Switched Voice Services (including Calling Cards and Toll-Free Services) .....	29
2.5.1	General Service Description .....	29
2.5.2	Switched Voice Service .....	29
2.5.3	Calling Cards.....	29
2.5.4	Toll Free Services .....	29
2.5.5	Service Operations .....	29
2.5.6	Service Performance .....	30
2.5.7	Service Maintenance .....	30
2.6	Corporate Network Routed Data .....	30
2.6.1	General Service Description .....	30
2.6.2	Service Operations .....	32
2.6.3	Service Performance .....	32
2.6.4	Service Maintenance .....	32
2.7	Layer 2 Virtual Private Network (L2VPN) Service .....	34
2.7.1	General Service Description .....	34
2.7.2	Service Operations .....	35
2.7.3	Service Performance .....	35
2.7.4	Service Maintenance .....	36
2.8	International Services.....	36
2.8.1	General Service Description .....	36
2.8.2	Service Operations .....	36
2.8.3	Service Performance .....	37

2.8.4	Service Maintenance .....	37
2.9	Custom Services.....	37
2.9.1	General Service Description .....	37
2.9.2	Service Operations .....	37
2.9.3	Service Performance .....	37
2.9.4	Service Maintenance .....	37
2.10	Network Time Protocol (NTP) Service .....	38
2.10.1	General Service Description .....	38
2.10.2	Service Operations .....	39
2.10.3	Service Performance .....	39
2.10.4	Service Maintenance .....	39
2.11	Network Security Monitoring Services .....	39
2.11.1	General Service Description .....	39
2.12	DDI Service: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM) .....	39
2.12.1	General Service Description .....	39
2.12.2	Service Operations .....	40
2.12.3	Service Performance .....	41
2.12.4	Service Maintenance .....	43
2.13	Data Center Network and Security Services (DCNSS) .....	43
2.13.1	General Service Description .....	43
2.13.2	Service Operations .....	44
2.13.3	Service Performance .....	44
2.13.4	Service Maintenance .....	44
2.14	Service Design and Development Lab (SDDL).....	45
2.14.1	General Service Description .....	45
2.14.2	Service Operations .....	45
2.14.3	Service Performance .....	46
2.14.4	Service Maintenance .....	46
2.15	DTV Support Services .....	46
2.15.1	General Service Description .....	46
2.16	Russian Services .....	48
2.16.1	General Service Description .....	48
2.16.2	Service Operations .....	49
2.16.3	Service Performance .....	49
2.16.4	Service Maintenance .....	50
2.17	Federal Relay Service .....	50
2.17.1	General Service Description .....	50

2.17.2	Service Operation.....	51
<b>3.</b>	<b>CSO Local Area Network (LAN) Service .....</b>	<b>51</b>
3.1	Corporate LAN Service .....	52
3.1.1	General Service Description .....	52
3.1.2	Service Operations .....	52
3.1.3	Service Performance .....	52
3.1.4	Service Maintenance .....	52
3.2	NASA LAN IP Management .....	52
3.2.1	General Service Description .....	52
3.3	Remote Access Services (RAS).....	53
3.3.1	General Service Description .....	53
3.3.2	Service Operations .....	53
3.3.3	Service Performance .....	53
3.3.4	Service Maintenance .....	53
3.4	Guest Network Services.....	53
3.4.1	General Service Description .....	53
3.4.2	Service Operations .....	54
3.4.3	Service Performance .....	54
3.4.4	Service Maintenance .....	54
<b>4.</b>	<b>Mission Network Services.....</b>	<b>54</b>
4.1	Mission - Data Transport Services.....	54
4.1.1	General Service Description .....	55
4.1.2	Legacy Mission Routed Data Services .....	58
4.1.3	Mission Network Security Policy .....	58
4.1.4	Service Demarcation Points .....	58
4.1.5	Service Performance .....	58
4.1.6	Real Time Critical Service Performance.....	58
4.1.7	Mission Critical Service Performance .....	59
4.1.8	Operations / Trouble Reporting .....	59
4.1.9	Service Performance .....	59
4.1.10	Service Maintenance .....	60
4.1.11	Mission Network Management .....	60
4.1.12	Legacy Mission Routed Data Transport Service – Security Suite .....	60
4.1.13	Legacy Mission Dedicated Data Service .....	60
4.1.14	Specific Service Description .....	60
4.1.15	Service Performance Category.....	61

4.1.16	Legacy Mission Dedicated Data - Real Time Critical .....	61
4.1.17	Legacy Mission Dedicated Data - Critical .....	61
4.1.18	Legacy Mission Dedicated Data Service – Custom .....	62
4.1.19	Service Maintenance .....	62
4.1.20	Mission Network Management .....	62
4.2	Dedicated Mission Voice Service .....	63
4.2.1	General Service Description .....	63
4.2.2	Service Operations/Trouble Reporting .....	63
4.2.3	Service Performance .....	64
4.2.4	Service Maintenance .....	64
<b>5.</b>	<b>NICS provided Center and Component Facility Services .....</b>	<b>65</b>
5.1	Cable Plant Services .....	65
5.1.1	General Service Description .....	65
5.1.2	Service Operations .....	65
5.1.3	Service Performance .....	66
5.1.4	Service Maintenance .....	66
5.2	Emergency Warning System .....	66
5.2.1	General Service Description .....	66
5.2.2	Service Operations .....	66
5.2.3	Service Performance .....	66
5.2.4	Service Maintenance .....	66
5.3	Public Address System .....	67
5.3.1	General Service Description .....	67
5.3.2	Service Operations .....	67
5.3.3	Service Performance .....	67
5.3.4	Service Maintenance .....	67
5.4	Radio Services .....	67
5.4.1	General Service Description .....	67
5.4.2	Service Operations .....	67
5.4.3	Service Performance .....	67
5.4.4	Service Maintenance .....	68
5.5	Telephone Services .....	68
5.5.1	General Service Description .....	68
5.5.2	Service Operations .....	68
5.5.3	Service Performance .....	68
5.5.4	Service Maintenance .....	68

5.6	Voice over Internet Protocol (VoIP).....	68
5.6.1	General Service Description .....	68
5.6.2	Service Operations .....	68
5.6.3	Service Performance .....	69
5.6.4	Service Maintenance .....	69
5.7	Cable Television Services.....	69
5.7.1	General Service Description .....	69
5.7.2	Service Operations .....	69
5.7.3	Service Performance .....	69
5.7.4	Service Maintenance .....	69
<b>6.</b>	<b>How to Request Services.....</b>	<b>70</b>
6.1	General.....	70
6.2	The Requirements Process.....	70
6.2.1	Customer Actions.....	70
6.2.2	NASA Communications Service Office (CSO) Actions .....	71
6.3	Rough Order of Magnitude (ROM) Costs and Detailed Cost Estimates .....	71
6.3.1	Detailed Cost Estimate vs. Rough Order of Magnitude (ROM) Cost...71	
6.3.2	Rough Order of Magnitude (ROM) Cost.....	71
6.3.3	Detailed Cost Estimate.....	71
<b>7.</b>	<b>Communication Services Office (CSO) FUNDING METHODOLOGY .....</b>	<b>72</b>
7.1	Customer Billing Assumptions FY15 Bill and FY16-FY20 Projected Billing: ....	72
7.2	CSO FY16 Funding Strategy:.....	74
	<b>Appendix A Supported Interfaces and Protocols .....</b>	<b>79</b>
	<b>Appendix B CSO Service Planning Timeframes.....</b>	<b>80</b>
	<b>Appendix C NASA CSO Points of Contact (POC) .....</b>	<b>82</b>
	<b>Appendix D Key Personnel .....</b>	<b>83</b>
	<b>Appendix E NAMS Instructions for Access to CSO/NICS SharePoint .....</b>	<b>84</b>
	<b>Appendix F Abbreviations and Acronyms .....</b>	<b>85</b>
	<b>Appendix G Glossary.....</b>	<b>91</b>
	<b>Appendix H NASA CSO IT Security Check Lists .....</b>	<b>94</b>

## List of Tables

Table 3 Performance Standards for IP Routed Data (by Service Category).....	32
Table 4 Performance Standards for L2VPN (by Service Category) .....	35
Table 5 Availability and Service Requirements for DDI.....	41
Table 6 Performance Response Times for IPAM.....	42
Table 7 DCNSS Service Performance Parameters .....	44
Table 8 Russia IT Services and Performance Standards .....	49
Table 9 Performance Standards for IP Routed Data (by Service Category).....	59
Table 10 Performance Standards for Mission Dedicated Data (by Service Category).....	62
Table B-1 CSO Service Planning Timeframes .....	80

# Communications Service Office (CSO) Services Document (CSD)

## 1. Introduction

### 1.1 Purpose

The purpose of this document is to furnish CSO Customers and users with a description of communications services available through CSO. Services are organized in two broad classifications of 1) spacecraft control and spaceflight support (Mission services), and 2) NASA Corporate communications support services.

Mission services are described in Section 4 and include Routed Data services, Mission Voice services, and custom data services supporting mission operations control centers and satellite tracking operations for spacecraft control; and spacecraft development and testing.

Corporate services are described in Section 2, 3 and 5, and include wide-area networks, center local-area networks, collaboration tools (video and audio), voice services, and other services for some Centers (for example cable plant, emergency warning and public address systems, radio, and phone systems). Specific services supported in Russia are found in Section 2.

This document also provides performance metrics and standard lead time information associated with these services and describes the processes to be followed for initiating CSO Service Requests (SRs) to the appropriate organization(s).

### 1.2 Scope

This document encompasses all the information that a user of CSO services may need to request services. The requirements submission processes described in this document are consistent with and part of the larger processes whereby the officials in charge of NASA Mission Directorates, Mission Support Offices, Program Offices, and the Directors of NASA Centers and Field Installations submit their requirements in support of Human Space Flight (HSF) Missions and non-Human Space Flight, sub-orbital and aeronautical Missions.

### 1.3 Document Organization

This document is organized as follows:

- Section 1 contains introductory information.
- Section 2 through 5 contains information on CSO's standard commodity and custom service offerings.
- Section 6 contains information on how one requests services from the CSO organization.
- Section 7 contains information on the methodology to be used in pricing and charging for services.
- Appendix A contains information on supported interfaces and protocols.
- Appendix B contains information on CSO Service Standard Intervals.

- Appendix C contains CSO Point of Contact (POC) information.
- Appendix D contains listings of key personnel.
- Appendix E contains NAMS instructions for access to CSO/NICS Sharepoint
- Appendix F contains a list of Abbreviations and Acronyms.
- Appendix G contains a Glossary of terms.
- Appendix H contains a link to the CSO Security Checklists.

#### 1.4 Related Documents

The following documents have been determined to be either applicable or have been referenced in the context of CSO. Where a document is known to be available on-line, a hyperlink to that document has been established.

##### 1.4.1 Applicable Documents

Applicable documents are those which by virtue of their inclusion in this paragraph become part of this document. Additionally, they have the same force and authority as if physically reproduced and incorporated as part of this document.

- A. NASA Policy Directive (NPD) 2800.1B, Managing Information Technology, expires July 21, 2015 and subsequent revisions.  
[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PD\\_2800\\_001B\\_&page\\_name=main&search\\_term=NPD%202800%2E1](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2800_001B_&page_name=main&search_term=NPD%202800%2E1)
- B. NPD 2810.1D, NASA Information Security Policy, expires June 09, 2015  
[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PD\\_2810\\_001D\\_&page\\_name=main&search\\_term=NPD%202810%2E1](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2810_001D_&page_name=main&search_term=NPD%202810%2E1)
- C. NASA Procedural Requirement (NPR) 2810.1A, Security of Information Technology, expires May 16, 2016  
[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PR\\_2810\\_001A\\_&page\\_name=main](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2810_001A_&page_name=main)
- D. NASA Policy Directive (NPD) 2540.1G, Personal Use of Government Office Equipment including Information Technology, expires June 08, 2015  
[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PD\\_2540\\_001G\\_&page\\_name=main&search\\_term=NPD%202540%2E1](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2540_001G_&page_name=main&search_term=NPD%202540%2E1)
- E. NPR 2830.1A NASA Enterprise Architecture Procedures, expires December 19, 2018  
[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PR\\_2830\\_001A\\_&page\\_name=main&search\\_term=NPR%202830%2E1](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2830_001A_&page_name=main&search_term=NPR%202830%2E1)
- F. NISN-Standard Operating Procedure (SOP)-0002, CSO SOP for Trouble Reporting, Activity Scheduling, Mission Freeze and Major Outage Notifications Effective November, 2007 Revision
- G. NPD2190.1B, NASA Export Control Program expires June 20, 2017

[http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal\\_ID=N\\_PD\\_2190\\_001B\\_&page\\_name=main&search\\_term=2190%2E1B](http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2190_001B_&page_name=main&search_term=2190%2E1B)

H. Federal Information Security Management (FISMA) Act of 2002

<http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

## 1.5 CSO Organization and Functions

In accordance with established organizational structures, the NASA CSO is under the direct governance and management control of the NASA Office of the Chief Information Officer (OCIO).

The I3P Program is intended to provide agency-wide management, integration, and delivery of IT infrastructure services. It is initially provisioned and supported via five major IT service acquisition contracts of which the NASA Integrated Communications and Services (NICS) is one.

The NICS Contract consists of program management, provisioning, and support of enterprise-wide and center and facility specific telecommunications, networking, security services, and collaboration services. NICS will provide infrastructure projects and services that are uniquely tailored to specific customer communities. These requirements are currently provided by multiple center-specific and enterprise-wide contracts across the agency. Additionally, the CSO holds master agreement/delivery orders (MA/DOs) on the General Services Administration (GSA) Networkx contracts. These MA/DOs include NASA-specific requirements for telecommunications services.

Initially, the NICS contract will be the primary replacement vehicle for obtaining delivery of communications Services across the Agency.

The CSO will be the focal point for management and business activities of all OCIO offered communications services. The CSO is based on a shared cooperative accountability model with three NASA Centers providing the required support to effectively and efficiently deliver service support. Contract administration and financial management shall be performed initially by the Marshall Space Flight Center (MSFC). Service management and service delivery oversight shall be provided by the CSO comprised of civil servants and contractors located primarily at MSFC, GSFC, and ARC. The management of technical operations shall be performed by the CSO staff with direct oversight and guidance of the Host Center CIOs and strategic input from the OCIO Communications Service Executive. The host centers' CIOs and Communications Service Executive will collaborate on issues pertaining to technical operations and the management of personnel will be performed by the host center CIO for staff at his/her center.

An Executive Steering Committee comprised of the ARC, GSFC, and MSFC host centers' CIOs will ensure integration of the multi-center Communications Service Office and provide recommendations to the Communications Service Executive (SE) on technical and service improvements. The Communications Executive Steering Committee composition, roles and responsibilities shall be detailed in the group charter.

This construct of shared accountability is intended to help the Agency achieve increased efficiency and reduce costs through standardization and commonality, while providing the means to build specialized solutions when mission needs require them.

Services provided include

- Integrated, end-to-end service provisioning
- Infrastructure, and supporting services for NASA's corporate local area networks (LANs) and wide area networks (WANs)
- Corporate voice and collaboration services
- Wide area and local mission services (voice, video, data)
- Center/facility and customer unique services
- Associated functions necessary for strategy generation
- Customer relationship, service management, operations, and security
- Integration functions in support of NASA's use of GSA contracts.
- Implementation for policies and guidance of the NASA OCIO in the management and delivery of Communications Services.

## 1.6 Standard Practices

### 1.7 General

CSO provides communications and networking services to its Customers. Domestic services shall, in so far as they are available, be obtained as standard commodity services. International services shall be obtained by making use of existing contract vehicles, by individual competitive procurements, or via agreements with international partners.

#### 1.7.1 Guidelines

CSO practices are governed by the following guidelines:

- a. It is the goal of NASA to provide communications in support of Mission and non-Mission activities at a minimum total cost consistent with requirements for capacity, performance, efficiency, reliability and security in accordance with applicable regulations.
- b. NPR 2830.1 NASA Enterprise Architecture Procedures requires NASA to ensure that IT expenditures are aligned with Agency goals, while reducing unnecessary duplication of resources. This NPR also requires that IT providers document their current state, future state, and plan to migrate to the future state, from an architectural standpoint. CSO's services were EA-approved in April 2006, and are updated as required.
- c. Local standards and/or architectures may be implemented to the extent that there is no conflict or incompatibility with Federal or NASA standards and/or the CSO approved EA. The proposed local standard and/or architecture shall have the concurrence of the Center CIO Representative which ensures that there are no incompatibilities or conflicts with existing Federal or NASA standards and/or approved EAs.
- d. NASA security policy forbids the unauthorized access to all Network systems and requires appropriate management controls to assure that all use of NASA communications assets are in pursuit of official Government activities. Management controls shall effectively prevent unauthorized traffic.

## 1.7.2 Acceptable Use Policy

The following Acceptable Use Policy, along with the official NASA policy on IT Security (ITS) and relevant U.S. federal laws, comprises the basic doctrine of the CSO Program.

### 1.7.2.1 Summary

- a. CSO supports all NASA Mission Directorates, Programs, Projects and Field Centers.
- b. CSO is not to be used for private gain or profit.

### 1.7.2.2 Specific

- a. Use of CSO services shall be in support of official NASA programs. All user requests for CSO connectivity shall be validated and supported by a Communications Subject Matter Expert (SME) or a Customer Commitment Manager (CCM).
- b. Use of CSO resources to support coordination and administrative execution of NASA business is permissible.
- c. Use of CSO resources to support NASA Missions, research, related training and associated technical activities at non-profit institutions of research and education is acceptable.
- d. Use of CSO resources for commercial or intellectual gain by for-profit organizations is not acceptable, unless those organizations are using the services to satisfy specific NASA contract or grant requirements.
- e. Use of CSO resources for research or education at for-profit institutions shall be reviewed on a case-by-case basis to ensure consistency with NASA programs. Lack of program approval shall result in a denial of service implementation or disconnection.
- f. Use of CSO resources to gain unauthorized use of resources attached to the NASA network may result in disconnection and legal prosecution.
- g. Use of CSO resources for the introduction of worms, viruses, trojans or other software that maliciously interferes with NASA operations is unlawful.
- h. Users shall place particular emphasis on restricting their disclosure of data and information to those persons who have a “need-to-know” for the data in order to perform their official duties.
- i. Users shall not attempt to access any data or programs contained on the NASA network for which they do not have authorization or explicit consent from the owner of the data or program, the CSO Project Manager or the CSO ITS Manager.
- j. Users shall not divulge dialup or dial-back modem phone numbers to unauthorized users.
- k. Users shall not divulge Internet Protocol (IP) addresses, computer names or any security vulnerabilities associated with a computer system to unauthorized users..
- l. Users shall not share account(s).
- m. Users shall not purposely engage in activity with the intent to:
  - 1) Harass other users

- 2) Degrade the performance of systems
  - 3) Deprive an authorized CSO user of access to a CSO resource
  - 4) Obtain resources beyond those allocated
  - 5) Circumvent CSO security measures
  - 6) Gain access to a CSO IT resource for which proper authorization has not been given
- n. Electronic communication facilities (such as E-mail, newsgroups or Internet) are for authorized government use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to, or over, nor stored on CSO resources.
- o. Users shall use the appropriate CSO service that meets security and operational requirements of the program data to be transferred.

### 1.7.3 Security

The objective of NASA security policies is to assure the confidentiality, integrity and availability of NASA IT resources. These policies preclude deliberate or accidental corruption of IT resources, protect information from unauthorized disclosure and ensure that disaster recovery and contingency planning (as defined in the Office of Management and Budget Circular A-130) is incorporated for all IT resources. CSO also utilizes NIST 800-53 recommended security controls for IT systems. CSO Customers will be required to submit an IT security checklist prior to connection to the NASA network. CSO coordinates and manages continuous monitoring efforts to ensure that systems meet FISMA, NIST and NASA Agency requirements to maintain and or obtain ATO (Authorization to Operate) and incorporate the overall lifecycle of design, acquisition implementation, maintenance, and disposal of architectures, systems, and devices supporting the communications needs of NASA.

#### 1.7.3.1 Information Confidentiality

CSO security procedures place significant emphasis on protecting Customers' unique information requirements. This focus is predicated on the following:

- A Customer's security level within the CSO shall be based on the sensitivity level given to the information. The productivity associated with that information should only be marginally affected by security safeguards required for protection and the information's degree of sensitivity.
- A Customer's communication access shall be based on the premise that what is not expressly permitted is prohibited.

Customer-focused security procedures shall include the reporting and subsequent handling of violations, and accountability for any access controls requested.

### 1.7.3.2 Internal Safeguards

CSO internal security policies shall adhere to the following principles and practices:

- a. Sensitivity levels shall be used to minimize the impact of failures in the network
- b. Customers shall be afforded the least access consistent with their requirements
- c. Technical controls, such as access lists, packet filters, firewalls and intrusion detection systems shall be employed to ensure that trust is not violated
- d. Remote access to the network shall be permitted, but only in conformance with network policies and practices governing such accesses
- e. CSO shall actively manage firewalls both by technical means and human oversight

### 1.7.4 CSO Support Applications

Information concerning CSO applications available to Customers, including access information, is available at the CSO Web site: <https://cso.nasa.gov>. A brief definition of these applications is shown below:

- a. Activity and Outage Posting Notification System (AOPNS): Provides an active key word and/or key phrase email subscription capability for receiving CSO activity and outage notifications. [Subscribe here](#)
- b. Call Detail: Provides billing information for switched voice services. The information is available by month, NASA location, and frequency.
- c. Mission Outage Notification System (MONS): Provides an active key word and/or key phrase email subscription capability for receiving CSO Mission services outage notifications. [Subscribe here](#)

### 1.8 Services

The NASA CSO operates Wide Area Network (WAN) services, LAN services, and unique Center and Component facility services that support both Corporate and Mission requirements. While the IT characteristics of these two types of requirements are similar, the Mission requirements have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that the policy executing in the Mission Network has a direct effect on the physical world, including significant risk to the health and safety of human lives and serious damage or loss of spacecraft.

In addition to WAN, LAN, and Center unique facility services the CSO provides Custom services. Custom services are those services that require additional engineering prior to ordering or providing the service. CSO can supply custom services tailored to fit a Customer's requirements; however, the Customer will be charged the additional costs that are associated with implementing and sustaining the customized solution.

Regardless of the method of delivery the CSO interfaces shall conform to American and International standards commonly accepted within and supported by industry. Procured

equipment and software are, wherever possible, to be available on a Commercial-Off-the-Shelf (COTS) basis. Communications circuits are procured using General Services Administration (GSA) contracts and centralized billing wherever possible.

The provisioning of CSO services entails certain lead times. Appendix B contains a specific discussion of lead times, based on different scenarios, which are intended for use as planning guidelines only; it is entirely possible that similarly appearing requirements have distinctive aspects that may increase or decrease the actual lead times from those shown.

### **1.8.1 Planning for Products and Services**

Quality planning is that systematic process that translates services into measurable objectives and requirements, and lays down a sequence of steps for realizing them within a specified timeframe. Quality planning is required before new services or processes are implemented, and may take place as a design project, using NASA Procedural Requirement 7120.7, or according to the established Service Request (SR) Process. During this planning, management or assigned personnel identify:

- The quality objectives and requirements for the service, considering such aspects as service and personal safety, reliability, availability and maintainability, production and inspection, suitability of parts and materials used in the service, selection and development of software, and recycling or final disposal of the service elements at the end of its life.
- Processes, documentation and resources required throughout the lifecycle
- Verification, validation, monitoring, inspection and test activities specific to the service and the criteria for product acceptance
- Records needed to provide evidence that the processes and service meet requirements
- Resources necessary to support operation and maintenance of the service
- Configuration Management appropriate to the service

### **1.8.2 Service Implementation Test and Acceptance**

CSO performs testing during service implementation to verify service delivery. The testing performed by CSO normally falls within two categories:

- a. Testing of purchased services such as carrier provided circuits
- b. Testing of services provided by the existing CSO infrastructure such as Mission and Corporate routed IP data, voice, and video.

When implementing new services, CSO works with the requesting Customer organization to verify, as closely as practical, the true end-to-end service delivery before agreeing that the Service Request is “in service”. In instances where the Customer is not prepared to test the service at implementation, CSO shall perform testing consistent with the type of service requested and the corresponding performance parameters as described elsewhere in the CSD for each category of service.

### 1.8.3 CSO Value-Added Services

In support of the direct services CSO provides to its Customers, there are numerous value-added services. Many are additional resources for the Customer's use, while others may be transparent to the user. These value-added services are part of the normal day-to-day support work performed by the CSO organization. They augment the primary Customer services and help to provide the continuing quality of the direct services available to our Customers. Some of these services are:

- Problem identification and resolution
- 24 x 7 Tier II Help Desk (NISC/GCC)
- NASA Teleconferencing Center (NTC) Tier II support 0600 – 1800 M-F (after hours as required or scheduled)
- Real time network monitoring
- Automated outage notifications
- Incident management
- Dedicated Customer Service Representatives (CSR)
- Dedicated Center Service Delivery Managers (CSDM)
- CSO Mission Service Managers (MSM)
- Multi-vendor service provisioning and coordination
- Requirements analysis and integration
- Rough Order of Magnitude (ROM) costing
- Project service level management
- Sustaining engineering
- Hardware and software maintenance
- NPG2810 compliance
- CSO Assessment and Accreditation (A&A)
- Customer forums
- Property management
- Contract management
- Virtual modeling for conference rooms
- Network integration and consulting
- Transition of applications and protocols to the CSO operational network
- Maintenance and operations of CSO laboratories
- Interconnection of CSO and non-CSO laboratories for collaborative research and prototyping

- Development of engineering expertise in emerging systems and technologies
- Coordination with the Agency Security Operations Center (SOC) for 24X7 Intrusion Detection
- Customer training
- Strategy generation and technology innovation

## 2. Corporate Network Services

### 2.1 Video Teleconferencing Services (ViTS)

Collaboration Services is responsible for the room equipment, operations, and the scheduling of Video Teleconferencing Services, but is not responsible for transport of the data. Rooms in which the ViTS systems will reside are provided by the NASA Locations, and physical changes to the rooms to support the ViTS are completed by the facilities organizations at the resident center. Collaboration Services coordinates with the appropriate service organizations to ensure the communication connectivity to the ViTS rooms is provided.

#### 2.1.1 Service Description

The Communications Services Office (CSO) Video Teleconferencing Services (ViTS) was established to provide videoconferencing solutions and services throughout the NASA Agency, including NASA contractors, Department of Defense, Educational and Professional Institutions, and NASA partners around the globe.

CSO ViTS Services include engineering, provisioning, installation, and maintenance of Agency wide videoconferencing facilities and the network infrastructure that support the video bridging operations supporting multipoint conferencing.



The NASA Teleconferencing Center (NTC), located at MSFC, is responsible for scheduling bridging services, monitoring video bridging operation and collecting metrics for the ViTS usage. The NTC also provides support for special events such as setting up conferences between the space station and educational facilities and linking global Space Agencies together for videoconferencing. To view CSO's NTC scheduling procedures, or to learn more about ViTS, please refer to the Video Conferencing Home Page at:

<https://cso.nasa.gov/content/video-teleconferencing-services-vits-1>

The video conferencing center has no call capacity or duration limitations. In order to establish your own video conference calls, you must request a NASA Resource Scheduler (NRS)

account. Once established, you may schedule your video conferences and audio-only add-ons through NRS - if you need assistance or have any questions, please contact the NTC.

### 2.1.2 ViTS Interface Types

CSO ViTS is based upon IP technology and supports International Telecommunication Union (ITU) compression standards such as H.323, H.320, H.264, H.263, G.728, and Siren. All new requests for ViTS services will be implemented with an IP interface connection allowing for services that are bandwidth dependent, such as High Definition (HD) ViTS. ViTS facilities connected via IP are capable of supporting point-to-point calls ranging from 384 kbps to 4.0 Mbps. The maximum bandwidth for multipoint calls can be configured at 8.0Mbps (supporting four (4) party HD ViTS). Legacy equipment as well as ISDN BRI/PRI will be supported as technology allows.

### 2.1.3 ViTS Facilities

ViTS Facilities are both Core and Customer funded, and consist of Custom Conference Rooms, Multi-Media facilities, and ViTS Roll-About (VRA) Systems. For on-demand conferencing, these facilities have built-in bridging support allowing up to three additional participants to be added to the call. Extended multipoint license can be purchased to increase the limit from three participants to seven participants.



Additional capabilities exist within each facility for supporting graphics, external video sources, as well as audio add-on support.

### 2.1.4 CSO Core Conference Rooms

These are Full-Service Conference Rooms located at each NASA Center and selected Associated Facilities that are typically operated by Center/Associated Facility provided room operators. These rooms are normally used for medium to large videoconferences and can accommodate 15 – 50 persons.



### 2.1.5 Custom Conference Rooms

**2.1.5.1** These are typically Full-Service Customer funded Conference Rooms, used for large videoconferences, and multimedia presentations, that can accommodate 30-200 persons. A new Custom Conference Room is designed to the Customer's specification. Standard capabilities include HD dual flat panel displays and/or projection systems.



Digital Video Disc (DVD) recorder, HD Digital Video Recorder (DVR), and front and rear cameras. Additional features include lighting/shade control, and computer interface pop-ups.

CSO custom conference rooms provide integrated control systems that automate and simplify advanced functions. Utilizing a control panel with custom GUI provides the User with ease of operation. Control systems are designed from a standard template providing continuity Agency wide.

### 2.1.6 Multimedia Systems

Multimedia systems are considered Custom, and generally accommodate 30-200 persons. A new Multimedia Conference Room is designed to the Customer's specification, and generally includes audio, with multimedia interfaces and displays. Control systems are an option of this service.

### 2.1.7 High Definition ViTS Roll-About (VRA) Systems

Single or dual screen VRA systems are cart mounted, and designed for smaller conference facilities. They generally support 3-30 persons. VRAs can be integrated with existing voice conferencing hardware or, with the addition of a phone line, provide audio add-on capability directly from the unit itself. The displays have integrated ATSC/QAM tuners and speakers. The on-board MCU has the capability of supporting up to three additional calls. The VRA system comes with a standard configuration consisting of a display(s), single HD camera, video codec, tabletop audio/status phone, Blu-Ray player, UPS, and the A/V mobile cart. VRAs can be easily

relocated to different rooms that contain the proper network interface. These rooms are designed for user-friendly operations and do not require a dedicated room operator.

### 2.1.8 Operations

The use of CSO ViTS facilities is coordinated locally at each Center. ViTS Facilities have the capability to connect to other video conferencing facilities either within or outside NASA's ViTS Network. As required, some external or off-network ViTS connections can be coordinated with the NTC.

The NTC provides the following services:

- a. Provides accurate support to schedules and forecasts.
- b. Performs certification testing and registration for all new conference rooms, maintains all Customer Certification Test Plans and checklists, and maintains accurate site profiles and directories.
- c. Provides first line troubleshooting to isolate technical problems of network and teleconferencing equipment.
- d. Supports engineering with research, testing, and development for new capabilities and project implementations.
- e. Tracks problem trends of trouble tickets to provide feedback to Engineering.
- f. Manages all Instant Meeting accounts and conference cancellation tracking. The NTC also manages, maintains, and reports Customer and Carrier metrics.
- g. Manages, maintains, and reports Customer and Carrier billing.

### 2.1.9 Service Performance

The following lists the service level targets and expected performance of the ViTS service:

- a. At a minimum, the ViTS Conferencing Bridge (MCU) shall support up to 20 NASA community locations participating in 1 to 10 simultaneous and independent conferences. This includes Custom, VRA, and DVA systems.
- b. If endpoints are compatible with American Encryption Standards (AES), the infrastructure can support encrypted video calls.
- c. The mean time to restore network service for an in-progress conference shall be less than or equal to 4 hours.
- d. The mean time to restore service for non-conference impacting problems shall be less than 2 business days.
- e. Conference availability shall be at least 99.5 percent to include room systems, CSO provided transport, and multipoint control system.
- f. IP service shall be provided at the Corporate Premium Routed Data Service Level.

### 2.1.10 Service Maintenance

Maintenance of one Core Conference Rooms at each NASA center is provided by CSO. Maintenance for all other Teleconferencing rooms is Customer-funded. Labor for maintenance is CSO provided; though Customers will be asked to fund labor for major implementation projects. Customers are responsible for funding travel for their designated projects. ViTS rooms must be refreshed on schedule as provided by their initial installation package and have valid owner information in the correct PSLA to be supplied maintenance by CSO. All estimates for new installations and refreshes will include the full vendor available equipment warranties. All incidents involving maintenance should be reported via the Enterprise Service Desk (ESD). CSO/NICS will respond to these incidents and determine the problem for resolution of equipment provided by CSO/NICS.\*

\* Rooms that are “split configuration”, i.e. have equipment purchased by non-CSO/NICS contractor. This non-CSO/NICS equipment should be maintained by the customer and/or their specific contractor.

## 2.2 DeskTop Mobile ViTS (DMV)

### 2.2.1 Service Description

The DMV service provides a desktop video collaboration service that allows Users to share voice, video and data between NASA standards-based ViTS rooms and a wide range of cross-platforms that include various computer platforms and mobile devices. The current service is based on the Vidyo product and has the capacity to support up to 5000 hosted User accounts. Accounts are requested via the Enterprise Service Desk (ESD).

The DMV service provides the capability to chat within a conference and record a meeting (the audio, video and the content being shared).

The DMV service is available on PC or MAC platforms and the desktop plugin is available via the ACES Software Refresh Portal. A DMV account is only needed to host a DMV meeting. Participants attending a DMV meeting as a guest do not have to install the VidyoDesktop client software but will be prompted to install a browser plugin as they join the conference.

The DMV service is also available on iPhone and Android platforms via the VidyoMobile app that is available as a free download at the appropriate app store. Users can join DMV Vidyo conferences via mobile as a guest.

The DMV User’s guide is provided via email to all new account holders.

### 2.2.2 Operations

The DMV infrastructure will be operated and maintained by the NIC Collaboration Services group. Any activities will be scheduled according to standard CSO/NICS policies and all outages will be reported via the standard CSO/NICS policies.

### 2.2.3 DMV Incident Reporting

Incident related to the DMV service shall be reported to the ESD. If the ESD is unable to resolve the incidents, then it will be escalated to the NICS NTC for resolution.

### 2.2.4 Service Performance

- a) The mean time to restore network service for an in-progress conference shall be less than or equal to 4 hours.
- b) The mean time to restore service for non-conference impacting problems shall be less than 2 business days.
- c) Conference system availability shall be at least 99.5

### 2.2.5 Service Maintenance

The DMV service systems are maintained by CSO with Customer funding. Any maintenance activities will be coordinated and scheduled via the standard CSO/NICS Activity scheduling process.

## 2.3 Voice Teleconferencing System (VoTS)

### 2.3.1 Service Description

CSO provides the audio meeting and conferencing needs of the Agency. This service includes the provisioning and maintenance of large room audio conferencing systems.

The VoTS audio bridging service provides reservation and reservationless service levels. Each service level is separated by specific features available and whether or not operator assistance is provided.

Depending on the service level selected, additional features such as conference recording, transcription and attendees lists are available at an additional cost.



### 2.3.2 Premier

In a Premier conference, an Operator calls each participant approximately 10 minutes prior to the scheduled call time, and announces each participant into the conference. The Operator monitors the meeting for its duration and can be notified for assistance by using \*0 on the telephone keypad. This is the most expensive of all the conference service levels and as such should be used only for critical NASA conferences that require conference monitoring and/or controlled participation. This type of conference does need to be scheduled and failure to cancel a reservation at least 30 minutes prior to the scheduled start time will incur cancellation charges.

### 2.3.3 Standard

In a Standard conference, an Operator greets the NASA participants as they join the conference. The Operator frequently monitors the meeting and can be notified for assistance by using \*0 on the telephone keypad. The Standard Service level should be used for NASA conferences that require limited conference monitoring and/or controlled participation. This type of conference does need to be scheduled and failure to cancel a reservation at least 30 minutes prior to the scheduled start time will incur a cancellation charge.

### 2.3.4 Instant Meeting

This is CSO's preferred service. The Instant Meeting is an Unattended Service that is available for use 24-hours a day, 7-days a week and does not require going through the reservation system after the initial set-up. It is the least expensive and cancellation fees do not apply. Each user is set-up with an account that provides them with a toll-free number. Participants dial into this conference using the toll free number and Personal Identification Number (PIN) provided by the Call Leader. Standard Instant Meeting accounts allow up to 300 participants. Call Leaders requiring more than 300 ports should contact the NTC at 1-877-857-NASA (857-6272). The Call Leader will need to provide justification for the request, and the request will need to be approved by the CSO Service Owner.

Instant meeting accounts are requested via the NAMS system and are available in three different types;

1. Domestic: allows toll free dialing to all CONUS and other domestic areas including Hawaii, Alaska, Canada, and US Territories (e.g. U.S. Virgin Islands, Guam, Puerto Rico).
2. Global: allows standard in-country toll and toll free dialing from all international locations except China, Brazil, Malaysia, India, Philippines, and Taiwan.
3. Global Enhanced: allows toll and toll free dialing from all Global locations including China, Brazil, Malaysia, India, Philippines, and Taiwan. This account has additional security restrictions including a 10 digit passcode, music on hold until the leader is present, and a mandatory post-conference report.

Instant meeting service information, including commonly asked questions can be found on the CSO website at [cso.nasa.gov](http://cso.nasa.gov)

## 2.4 Voice Teleconferencing System (VoTS) Facilities

VoTS room systems are differentiated by the number of participants supported (anywhere from 4-36 microphones). Typical system configuration consists of an audio mixer, mutable microphones, power amplifier, and speakers. Additional customization is available to meet specific Customer requirements. All Full Service ViTS rooms have VoTS service and VoTS can also be integrated with a Video Roll-About (VRA) system for video teleconferencing.

### 2.4.1 Operations

The following is an overview of the concept of operations.

### 2.4.2 VoTS Incident Reporting

#### a. During the Conference

During a voice conference, if a problem occurs, press \*0 to request the assistance of an Operator. The Operator shall enter the conference, attempt to resolve any technical problem and offer further assistance to the users.

#### b. After the Conference

If a problem occurred that prevented the successful completion of the conference to your satisfaction, [please](#) contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create an incident record and dispatch it to the appropriate support organization for resolution.

#### NOTE:

Using \*0 for Operator assistance during the conference does not report the problem to the ESD

### 2.4.3 Service Performance

Current performance parameters are in the following paragraph and in Table 1. As a minimum, the service shall support up to 350 NASA community users participating in up to 70 simultaneous and independent conferences. Service capacity is planned such that Denial of Service shall be less than 3 percent for any given 30-day period.

### 2.4.4 Service Maintenance

Voice conferencing systems are maintained by CSO with Customer funding. Technology upgrades of the rooms are the funding responsibility of the Customer.

*Table 1 VoTS Service Performance (by Service Category)*

<b>Service Category</b>	<b>Availability<sup>+</sup> (Percent)</b>	<b>Restoral Time<sup>→</sup></b>	<b>Coverage Period</b>	<b>Impacted Conferences</b>
<b>In progress conference</b>	99.95	4 hr <sup>→</sup>	6 a.m. Eastern Monday to 6 p.m. Pacific, Friday	< 9 per month
<b>Non-conference Impacting Problems</b>	N/A	<2 days	6 a.m. Eastern Monday to 6 p.m. Pacific, Friday	N/A

## 2.5 Switched Voice Services (including Calling Cards and Toll-Free Services)

### 2.5.1 General Service Description

NASA Switched Voice Services (SVS) are provided using this service. They include domestic and international long distance service from the desktop, telephone calling cards held by individuals, and toll-free in-bound services for NASA sites and selected contractor sites. The GSA Network contract is used to provide these services.

### 2.5.2 Switched Voice Service

Switched Voice Service is primarily used to provide voice service between NASA centers and to off net (non-NASA) locations, including international sites.

### 2.5.3 Calling Cards

Calling Cards are primarily used to provide Customers voice services while on official travel or in emergency situations.

### 2.5.4 Toll Free Services

Toll Free Services are primarily used to provide public and NASA personnel access to NASA information, access to remote electronic mail (e-mail), and voice mail and to contact service help desks around the Agency.

### 2.5.5 Service Operations

If a problem occurs with the Switched Voice Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create an incident ticket and dispatch it to the appropriate support organization for resolution

---

<sup>+</sup> The availability includes room systems, CSO provided transport and multiport control system.

<sup>→</sup> These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary and are mean time to restore figures.

**2.5.6 Service Performance**

The Long Distance (LD) service performance parameters will be consistent with the GSA Network contract terms. Current service performance parameters are listed in Table 2.

*Table 2 Performance Standards for Switched Voice*

Service Category	Availability+ (Percent)	MTTR+	Coverage Period	Probability Of Call Blockage
Switched Voice	99.5	< 4 hours→	24X7	<1% (P.01 or better)

**2.5.7 Service Maintenance**

Switched Voice Services are maintained by CSO and are provisioned as part of the service.

**2.6 Corporate Network Routed Data**

**2.6.1 General Service Description**

The Routed Data Service utilizes a backbone infrastructure. Routed data services include Corporate Local Area Network (LAN) services in addition to Wide Area Network (WAN) services. Agency policy dictates the use of IP as the Agency standard protocol for data networking; other protocols are supported on a legacy basis. A routed data tail circuit is required to provide access from a location remote from one of the NASA centers or CSO Hubs.

---

+ These values apply only for those parts of the WAN service supported by the CSO backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

→ These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary and are Mean Time To Restore (MTTR) figures.

### **2.6.1.1 Routing Protocols**

CSO currently supports several intra-domain routing protocols, including Static, Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), and inter-domain routing protocols such as Border Gateway Protocol (BGP). CSO engineers shall work with Customers to select a protocol consistent with both the Customer's requirement and the common network architecture.

### **2.6.1.2 Service Demarcation Points**

The Demarcation Point for CSO IP Routed Data Services shall be an 802.3 interface, as defined by the IEEE taskforce terminated on customer provided equipment. The LAN interfaces available include, but are not limited to; 10-Base-T, 100-Base-TX, 100-Base-FX, 1000Base-X (SX, LX, and ZX) and 10GBase-X Ethernet. Several legacy interfaces that have been deemed End of Sales shall continue to be supported until End of Life declarations are issued.

### **2.6.1.3 Corporate Routed Data Category Descriptions**

Two service performance categories for Corporate routed data services have been defined: (1) Premium, and (2) Standard. CSO expects that the definitions of these performance categories shall evolve as they are mapped against the existing and planned needs of our Customers. Note that requirements not satisfied by these performance categories may be supportable under a custom service. Networks comprised of different service performance categories can be installed at a Customer location to provide increased reliability.

Service performance metrics for the two categories of Corporate domestic IP routed data service are listed in Table 2 and 3.

### **2.6.1.4 Premium Internet Protocol (PIP) Service**

PIP service is differentiated from Standard Internet Protocol (SIP) service in that it provides a higher performance level, higher priority for problem resolution, and has limited connectivity to the general Internet.

PIP service is most appropriate for internal Agency networking requirements where the Agency's operations should be isolated from the general Internet and is used as a project specific resource.

### **2.6.1.5 Standard Internet Protocol (SIP) Service**

This service provides for basic data networking connectivity using the IP suite. SIP service is the commodity Internet service that provides the Agency's link to the Internet in general. It provides basic universal Internet connectivity with lower performance guarantees or restrictions on acceptable use.

SIP service is open to the public to enable access to publicly available NASA information sources such as Internet services.

**2.6.1.6 Internet Protocol (IP) Routed Data - Security**

While security is inherent in the definition of Mission Critical Service, security features can also be implemented within the context of Routed Data Service. For example, route and/or traffic filtering may be implemented to provide restricted access to certain sub-networks as indicated by Customer or IT Security (ITS) requirements. It is important to note that CSO views security as a responsibility that is shared with the Customer. CSO works with the Customer to identify potential threats and solutions for satisfying Customer needs.

New users or services must complete a NASA IT Security Checklist to connect to the network. The designated Customer Service representative will provide the Checklist.

**2.6.2 Service Operations**

If a problem occurs with the Routed Data Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution.

**2.6.3 Service Performance**

The performance specifications in Table 3 are stated from CSO-location to CSO-location, e.g., center-to-center, and these specifications apply to Continental United States (CONUS) connections only. The Customer is also advised that CSO cannot guarantee performance beyond CSO’s connections to the Internet.

**2.6.4 Service Maintenance**

Routed data services are maintained by CSO and are provisioned as part of the service.

*Table 3 Performance Standards for IP Routed Data (by Service Category)*

<b>Service Category</b>	<b>Availability<sup>+</sup> (Percent)</b>	<b>Restoral Time<sup>→</sup></b>	<b>Coverage Period</b>	<b>Acceptable Packet Loss (Percent)</b>	<b>Round Trip Time<sup>♦</sup></b>	<b>Maximum TransMission Unit (MTU) Settings (Bytes)</b>
<b>Premium</b>	99.99	4hr <sup>→</sup>	24x7	<0.001	<100 ms	1500

<sup>+</sup> These values apply only for those parts of the WAN service supported by the CSO backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

<sup>♦</sup> Round Trip Time (latency) is specified for data flow between domestic WAN nodes controlled and operated by CSO. Latency is a function of distance and carrier capabilities. User applications that are sensitive to latency shall be engineered to account for the upper limit round trip times specified in the above table.

<sup>→</sup> These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.

Service Category	Availability <sup>+</sup> (Percent)	Restoral Time <sup>→</sup>	Coverage Period	Acceptable Packet Loss (Percent)	Round Trip Time <sup>♦</sup>	Maximum TransMission Unit (MTU) Settings (Bytes)
		MTTR				
<b>Standard</b>	99.99	4 hr <sup>→</sup> MTTR	24x7	<0.001	<100 ms	1500

### 2.6.4.1 Internet Protocol (IP) Routed Data - Definition of Terms

#### 2.6.4.1.1 Availability

Service availability is measured over the period of one calendar month. Service availability excludes scheduled preventative maintenance or upgrades. The availability is calculated for the service as a whole and is the average availability between all service delivery points. CSO's approach to measuring availability includes the Customer's Service Access Point (SAP) as well as the availability of the shared resources within the network, i.e., the backbone.

#### 2.6.4.1.2 Time to Restore a Service

CSO shall make every effort through its contractors and carriers to restore interrupted service in a timely manner. A requirement has been levied by CSO on itself, its contractors and its carriers to return CSO services to an operational state as indicated in Table 2 and 3.

Premium Internet Protocol (PIP) and Standard Internet Protocol (SIP) time to restore is based on a calculated mean. Mean-Time-To-Restore (MTTR) for PIP and SIP services is calculated on outage data gathered in the proceeding 90 days and is based on the time CSO receives an outage notification to the time the service is restored. A mean time calculation can result in individual PIP or SIP service outages that exceed 4 hours respectively without exceeding the 4 hour MTTR.

Circumstances that can cause service outages to exceed the above limits are manmade and natural disasters such as destruction of facilities or cabling. Facility access restrictions or Customer directed delays could also cause service outages to exceed the above limits.

#### 2.6.4.1.3 Packet Loss

Packets transmitted from the source CSO/Customer interface, i.e., the connection between the CSO router and the Customer router, but not received at the destination CSO/Customer interface. Acceptable loss is measured over any 24-hour interval.

#### 2.6.4.1.4 Round-Trip-Time

Round Trip Time is measured by utilizing the Internet Control Message Protocol (ICMP) utility of Packet Inter-Network Groper (PING). Since PING utilizes TCP protocol 1; it has the lowest priority during transit across the network. This means that all other traffic receives a higher priority during queuing within the router on a network link. Because of this, an average is calculated to ensure that anomalies shall not skew the data. For the purpose of latency measurements, CSO uses an average of 100 packets each sent with a 36 byte payload.

#### **2.6.4.1.5 Maximum Transmission Unit (MTU)**

The Maximum Transmission Unit (MTU) is the maximum size of a single data unit (e.g., a frame) of digital communications. MTU sizes are inherent properties of physical network interfaces, normally measured in bytes. The current MTU settings are the current default on the core sections of the Corporate routed data network and are not the CSO default at the CSO Customer facing interface. Increases to the CSO Corporate routed data network default MTU sizing between CSO at the Customer demarcation point and the Customer CSO facing interface is increased on a case by case basis.

### **2.7 Layer 2 Virtual Private Network (L2VPN) Service**

#### **2.7.1 General Service Description**

The L2VPN Service utilizes an infrastructure that includes a CSO-managed backbone service. The L2VPN service is appropriate when the Customer requires transparent extension of LAN services between two physical locations. Unlike Corporate VPN service (under DCNSS), L2VPN does not provide data encryption. Use of L2VPN as a solution will be the decision of CSO based on established CSO and Agency policy. L2VPN service is offered only at established CSO backbone services locations.

##### **2.7.1.1 Service Demarcation Points**

The service demarcation point for the CSO L2VPN Service shall be the WAN core router interface of the CSO L2VPN equipment. The LAN interfaces available include, but are not limited to; 10-Base-T, 100-Base-TX, 100-Base-FX, 1000Base-X (SX, LX, and ZX) and 10GBase-X Ethernet. Several legacy interfaces that have been deemed End of Sales shall continue to be supported until End of Life declarations are issued. Layer 2 Virtual Private Network (L2VPN) Category Descriptions

CSO's L2VPN service is independent of the Premium and Standard IP (PIP/SIP) network service levels. However, the service levels provided meet PIP level agreements. CSO expects that the definitions of these performance categories shall evolve as they are mapped against the existing and planned needs of our Customers. Note that requirements not satisfied by these performance categories may be supportable under a custom service.

##### **2.7.1.2 Layer 2 Virtual Private Network (L2VPN) Security**

By definition, L2VPN services are restricted to defined source and destination parameters to limit access to certain sub-networks as indicated by Customer or IT Security (ITS) requirements. It is important to note that CSO views security as a responsibility that is shared with the Customer. CSO works with the Customer to identify potential threats and solutions for satisfying Customer needs using CSO's IT security checklists.

New users or services must complete a NASA IT Security Checklist to connect to the network.

## 2.7.2 Service Operations

If a problem occurs with an L2VPN service, contact the Enterprise Services Desk (ESD) at 1-877-677-2123, by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov) or via the web at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create a trouble ticket and dispatch it to appropriate maintenance agency for resolution.

## 2.7.3 Service Performance

The performance specification in Table 4 is stated from CSO-location to CSO-location (e.g., Center-to-Center) and these specifications apply to Continental United States (CONUS) connections only. The Customer is also advised that CSO cannot guarantee performance beyond their connections to the Internet.

### 2.7.3.1 Availability

Service availability is measured over the period of one calendar month. A failure is defined as an event that results in a loss of connectivity in excess of 5 seconds. Service availability excludes scheduled preventative maintenance or upgrades. CSO's approach to measuring availability includes the Customer's Service Demarcation Point (SDP) as well as the availability of the shared resources within the network (i.e., the backbone).

*Table 4 Performance Standards for L2VPN (by Service Category)*

Service Category	Availability <sup>+</sup> (Percent)	Restoral Time <sup>→</sup>	Coverage Period	Round Trip Time <sup>♦</sup>
L2VPN	99.99	4 hr <sup>→</sup>	24X7	<100 ms

### 2.7.3.2 Restoral Time

CSO shall make every effort through its contractors and carriers to restore interrupted service in a timely manner. A requirement has been levied by CSO on itself, its contractors and its carriers to return network services to an operational state as indicated in Table 2-4.

Restoral time is based on a calculated mean. Mean-Time-To-Restore (MTTR) for L2VPN services is calculated on outage data gathered in the proceeding 90 days and is based on the time CSO

<sup>+</sup> These values apply only for those parts of the WAN service supported by the CSO backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

<sup>♦</sup> Round Trip Time (latency) is specified for data flow between domestic WAN nodes controlled and operated by CSO. Latency is a function of distance and carrier capabilities. User applications that are sensitive to latency shall be engineered to account for the upper limit round trip times specified in the above table.

<sup>→</sup> These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.

receives an outage notification to the time the service is restored. A mean time calculation can result in individual L2VPN service outages that exceed 4 or 24 hours respectively without exceeding the 4- or 24- hour MTTR.

Circumstances that can cause service outages to exceed the above limits are manmade and natural disasters such as destruction of facilities or cabling. Facility access restrictions or Customer-directed delays could also cause service outages to exceed the above limits.

### **2.7.3.3 Round-Trip-Time**

Round Trip Time is measured, monitored, and managed by utilizing Cisco IP Service Level Agreement (IP SLA) tests that are generated between each Center. For the purpose of latency measurements, the network generates 1000 packets per minute to measure latency.

### **2.7.4 Service Maintenance**

L2VPN service level agreements are maintained through employing the appropriate maintenance levels for hardware components and elements that support the L2VPN services, e.g. Juniper depot maintenance agreements with 4 hour restoral and sub 4 hour parts replacement.

## **2.8 International Services**

### **2.8.1 General Service Description**

The International data distribution services are provided to many of NASA's International Partners and agencies through cooperative arrangements. Rather than purchase dedicated circuits for each requirement, cooperative consolidation and integration of various requirements into an economical infrastructure provides the basic connectivity for programmatic requirements for the transport of data, voice, facsimile, electronic mail, and video.

#### **2.8.1.1 Corporate Network**

Expansion of the Corporate Network International Services network is accomplished using one or more of the following approaches:

- a. Sharing CSO's backbone circuit extensions with International Partner Agency networks
- b. Providing CSO tail circuit extensions from a NASA site to an International Partner Agency location via a TIC location.
- c. Establishing research network or general internet peering arrangements

New users or services must complete a NASA IT Security Checklist to connect to the CSO IP networks.

### **2.8.2 Service Operations**

If a problem occurs with an International Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year

organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution

### **2.8.3 Service Performance**

There are no standard performance metrics for international services. Performance metrics for international services are dependent on the type of service requested and the ability of CSO and its providers to meet those requirements. The best possible Service Level Agreements (SLA) guarantees are provided to the Customer when all dependencies have been identified.

### **2.8.4 Service Maintenance**

International Services are maintained by CSO and are provisioned as part of the service

## **2.9 Custom Services**

### **2.9.1 General Service Description**

Custom telecommunication and networking services are specifically designed and engineered to meet unique NASA programmatic requirements. Each program determines the unique attributes of the data distribution services in such terms as security, availability, redundancy, and features that provide the optimum trade-off between cost and program success.

Custom Services may be used both for space flight Mission critical applications and for general administrative support requirements possessing unique attributes that would utilize the CSO's Corporate network.

### **2.9.2 Service Operations**

If a problem occurs with the Corporate Custom Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution

### **2.9.3 Service Performance**

There are no standard performance metrics for custom services. Performance metrics for custom services are dependent on the type of service requested and the ability of CSO and its providers to meet those requirements. The best possible Service Level Agreements (SLA) guarantees are provided to the Customer when all dependencies have been identified.

### **2.9.4 Service Maintenance**

Custom Services are maintained by CSO and are provisioned as part of the service

## 2.10 Network Time Protocol (NTP) Service

### 2.10.1 General Service Description

The Network Time Protocol (NTP) is an Internet Protocol that is used to synchronize a computer's clock to a reference time source. The NASA Communications Service Office (CSO) NTP Service provides Agency users with a stratum 1 NTP time reference source, available as a distribution service to Center and Project lower stratum level distribution servers, or directly to application/web/database servers and clients. The NASA CSO NTP servers respond to host polls with Coordinated Universal Time (UTC) timestamps with no offsets for any time zones. The NASA CSO NTP servers provide UTC which is adjusted for leap seconds.

The NASA CSO NTP service consists of servers accessible via the Premium IP (PIP) and Standard IP (SIP) networks at Marshall Space Flight Center, Goddard Space Flight Center, Ames Research Center, Kennedy Space Center and Johnson Space Center. Hosts located on any trusted NASA network may use the service by pointing to one or more of the following:

Location	SIP	PIP
ARC	time1a.nasa.gov	time1b.nasa.gov
GSFC	time2a.nasa.gov	time2b.nasa.gov
MSFC	time3a.nasa.gov	time3b.nasa.gov
KSC	time4a.nasa.gov	time4b.nasa.gov
JSC	time5a.nasa.gov	time5b.nasa.gov

Please note time1a and time1b pull from the same GPS time source (as do time2a and 2b, and time3a and 3b, etc.). Time1x, time2x, time3x, time4x and time5x all pull from different GPS time sources.

Typical use for application servers is to point directly to individual time servers (3 or more are recommended to allow an out-of-range time to be ignored) using the names above. Client systems may use a round-robin configuration, using a single entry of “time.nasa.gov” for clients to pull time regardless of location, as follows:

- Local (LAN) - time.nasa.gov points to a local AD source, if available. If an NTP server is not available locally, the query would proceed to the Agency (inter-Center) layer.
- Agency - time.nasa.gov points to a NASA CSO source (round-robins the ten NASA servers).
- Public - time.nasa.gov points to ntp.nasa.gov (managed out of Ames Research Center and available to the Internet public), which is an alias for time.nist.gov, time-a.nist.gov, and time-b.nist.gov.

Customers using the NASA CSO NTP service are encouraged to subscribe to the ntp-users@lists.nasa.gov at <https://lists.nasa.gov/mailman/listinfo/ntp-user> to receive service-related updates and activity notices.

### 2.10.2 Service Operations

If a problem occurs with the NTP Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution

### 2.10.3 Service Performance

There are no performance metrics for this service.

### 2.10.4 Service Maintenance

The CSO NTP Services are maintained by the CSO and are provisioned as part of the service.

## 2.11 Network Security Monitoring Services

### 2.11.1 General Service Description

The Agency Security Operations Center (SOC), located at the Ames Research Center (ARC), maintain security monitoring systems that are strategically deployed within CSO to provide NASA a monitoring capability to detect and respond to network intrusions, or unauthorized access/use of NASA networking resources. Each center is monitored via a security monitoring system, as well as each of the Internet peering locations.

The CSO Security team is located at the Marshall Space Flight Center. The SOC monitors all of the sensors across the network and contacts the affected center and/or CSO if an intrusion is detected. Daily SOC reports are generated and delivered to CSO Security and each center IT Security Manager with a summary of all attacks detected.

## 2.12 DDI Service: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM)

### 2.12.1 General Service Description

Through the DDI Service, CSO provides Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), Autonomous System Number (ASN) management and IP address management (IPAM), for all IP resources assigned to NASA. CSO serves as the Agency's authorized interface with the Regional Internet Registries, DOTGOV, and other registration authorities for management of IP address space and domain names, and delegates authority to local network management organizations for day-to-day management and monitoring of local IP resources, using the DDI system (application and data repository). DDI resource usage must follow the guidelines set forth in the document NITR-2830-1C, Networks Using NASA Internet Protocol (IP) Resources or NASA Physical Space on the NASA Communications Architecture Working Group (CAWG) Sharepoint site:

<https://sharepoint.msfc.nasa.gov/sites/cso/CAB/CAWG/default.aspx>

### **2.12.1.1 Domain Name Services (DNS)**

CSO registers NASA.GOV and other second-level domain names and administers NASA's Internet domain naming policies and conventions. Sub-domain management is conducted by the appropriate NASA centers/organizations. DNS activities supported include additions, removals, and changes to the DNS database, and coordination with registration authorities such as ARIN and DOTGOV. Web service policy is set by the Web Services Office (WSO) of the Agency Office of the Chief Information Officer (OCIO), and administered as applicable, by the CSO through the DDI service.

Creation of new second-level domains or NASA.GOV-level domain names shall require the approval of CSO and Agency Office of the CIO (OCIO) management in accordance with Agency policies.

### **2.12.1.2 Dynamic Host Configuration Protocol (DHCP)**

CSO provides the central management system for DHCP services across the Agency, and delegates the day-to-day management and monitoring of local DHCP services to all NASA Centers and approved projects.

### **2.12.2 Service Operations**

To request a new service or to report trouble with an existing service, refer to Section 6 in this document.

#### **2.12.2.1 Internet Protocol Address Management (IPAM)**

CSO provides top-level management of all IP address space and Autonomous System Numbers assigned to NASA. Local management organizations use the DDI system to catalog, monitor, and manage IP address ranges and ASNs assigned to that organization.

NASA IP address space includes any IP address assigned to the NASA Org ID with the Regional Internet Registries, such as the American Registry of Internet Numbers (ARIN) and the Reseaux IP Europeans (RIPE). CSO may assign NASA IP address space for NASA Customer use for the life of approved NASA projects. CSO retains management authority over the assignment of this address space assigned to Customers. Customers may not delegate the use of this address space to third parties. Customers must cease to use this address space upon the completion of the project it was intended to support subject to memorandum of agreement (MOA) to be executed upon assignment of the address space to the Customer.

Assignment of new IP address ranges and ASNs shall require the approval of CSO and Agency Office of the CIO (OCIO) management in accordance with Agency policies.

For additional guidance on the use of IPv6, refer to the NASA IPv6 Guidelines on the NASA Communications Architecture Working Group (CAWG) Sharepoint site:

<https://sharepoint.msfc.nasa.gov/sites/cso/cawg1/SitePages/Home.aspx>

### 2.12.3 Service Performance

General system availability is 24 hours/day x 7 days/week x 365 days/year, except during scheduled maintenance periods or outages announced in advance in the CSO Activity & Outage Posting and Notification System (AOPNS).

Central management is accomplished using a primary Executive Server and a backup Executive Server at a separate location. Local operations are supported, at a minimum, with a pair of redundant DNS and DHCP servers on each local area network. Inter-Center (Agency) services are provided with a total of four (4) servers distributed regionally within a single network hop of any NASA Center. Public (Internet) services are provided with a total of three (3) servers aligned with CSO Internet Peering Points. Recursion services are provided with a total of five (5) caching servers, located at CSO NASA Core nodes.

*Table 5 Availability and Service Requirements for DDI*

Item	Explanation	Objective
Wide Area Network service  Provided by CSO (CSO)	DDI traverses CSO's infrastructure for intra-and extra-Agency services, including the Internet.	Overall availability provided by CSO at 99.5%. Refer to the Routed Data section of this document for performance metrics associated with PIP and SIP routed data services.
Central System Availability  Provided by CSO	DDI system resources are deployed in a redundant configuration, with the primary central Server located at the MSFC NASA Data Center (NDC) on the MSFC DCNSS infrastructure, and a backup central server located on the GSFC DCNSS infrastructure. Disaster Recovery in the event of total WAN isolation for each local network shall be addressed by the local network management organization in compliance with the DDI Concept of Operations.	Overall, 99.99%. Refer to the DCNSS section of this document for performance metrics associated with network connectivity.

Item	Explanation	Objective
Local System Availability (DNS, DHCP)  Provided by local network management organization (CSO or other)	DDI local resources are generally deployed in a redundant configuration on each local network infrastructure. Local resources continue to operate even if isolated from the central Server.	System availability, 99.99%, subject to local network performance metrics.

### 2.12.3.1 Performance Response Time

Applications should not time-out due to system delays or produce performance impacts for users that result in the inability to meet user requirements in a timely manner. In particular, performance will be monitored for all DDI system components using logs and real time monitoring software. Expected performance is listed below in Table 6.

*Table 6 Performance Response Times for IPAM*

Transaction	Expected Performance
Intra-Agency DNS lookup	A recursive DNS server should not induce more than 50ms of lookup latency (i.e. round trip time for query and response) for LAN queries of resource records (RR) in local and Agency zones 99.9% of the time, not to exceed 1s.  <b>Exception:</b> some Mission networks include high-latency WAN components that exist only for telemetry and command & control. DNS response for clients at these sites may exceed these limits.
Extra-Agency DNS lookup	A recursive DNS server should not induce more than 500ms of lookup latency for popular Internet sites that are network accessible (e.g., www.google.com, www.microsoft.com, www.yahoo.com) even if the response is not cached locally, 99.9% of the time, not to exceed 2s.  <b>Exception:</b> some Mission networks include high-latency WAN components that exist only for telemetry and command & control. DNS response for clients at these sites may exceed these limits.

Transaction	Expected Performance
DNS Record Change Requests	Agency and Public DNS record change requests should be implemented within 1 business day of approval. Federal holidays and network freezes caused by major Agency events are excluded from this calculation. Local DNS record change requests are controlled by local management organizations (CSO or other).

#### 2.12.4 Service Maintenance

The DDI systems are maintained by CSO and are provisioned as part of the service. Local organizations provide touch support for equipment located on networks outside the CSO demarcation. Refer to the DDI Concept of Operations [DDI-007].

### 2.13 Data Center Network and Security Services (DCNSS)

#### 2.13.1 General Service Description

DCNSS provides a secure, highly available data center (centralized or distributed) networking infrastructure for computing systems and services that requires a redundant infrastructure managed at an Agency level. Customers are able to tailor their services based on a grouping of service options and levels that meet their projects/programs requirements.

- a. LAN connectivity for agency wide server applications
  1. Switch ports (100,1000, 10000Mbps)
  2. IP address assignment
  3. Domain Name Service
  4. Server network-based load balancing
- b. Network Security Services
  1. Firewall support
  2. Proxy server support
- c. WAN connectivity
  1. Direct connection to CSO WAN
  2. Network-to-Network Virtual Private Network (VPN) is provided by to other centers and partners. This service provides an encrypted tunnel between two networks. CSO's Network-to-Network VPN service supports the Advanced Encryption Standard (AES128, AES192, and AES256). The devices used are Federal Information Processing Standard (FIPS) 140-2 compliant.
  3. Client-to-Network VPN tunnels for system administrator access to server resources

As an extension to traditional CSO WAN services, DCNSS extends the network support to NASA Data Centers by providing the following three distinct networks

- a. Private Network – supports Data Center servers for Agency wide services not requiring Internet access
- b. Public Network – supports Data Center servers for Agency wide services intended to support services that extend beyond NASA to the Public Internet
- c. Demilitarized Zone (DMZ) Network – Provides a secure path for traffic flowing between the Private and Public networks and to the CSO WAN

**2.13.2 Service Operations**

If a problem occurs with the DCNSS Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution.

**2.13.3 Service Performance**

Current service performance parameters are shown in Table 7.

*Table 7 DCNSS Service Performance Parameters*

<b>Service Category</b>	<b>Availability<sup>+</sup> (Percent)</b>	<b>Restoral Time<sup>→</sup></b>	<b>Coverage Period</b>	<b>Acceptable Packet Loss (Percent)</b>	<b>All Standard Changes (e.g. port activation)</b>
<b>Premium</b>	99.99	4hr <sup>→</sup> MTRR	24x7	<0.001	
<b>All Services</b>					< 24 hrs.

**2.13.4 Service Maintenance**

DCNSS is maintained by CSO and is 100% Customer funded. Overall service costs are evaluated annually. The operations, refresh (5-7 year technology refresh model is used), and maintenance costs of the shared infrastructure components are distributed across the service’s customers.

---

<sup>+</sup> These values apply only for those parts of the WAN service supported by the CSO backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

<sup>→</sup> These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.

## 2.14 Service Design and Development Lab (SDDL)

### 2.14.1 General Service Description

The CSO Service Design and Development Lab (SDDL) provides an Agency-wide environment in support of the life cycle of service development, from concept, through prototype, into deployment, on-going service delivery, and decommission. The SDDL includes three types of environments:

1. CSO Prototyping Network (CPN): Closed Agency-wide lab environment. The CPN is used to test technologies, protocols, and equipment (collaborative or independent) before introduction into a production network. The CPN connects Center labs and other OCIO-sponsored labs using CSO's L2VPN WAN service. These labs must not connect to NASA production networks or the Internet.
2. Internetwork Lab (INL): Agency-wide lab environment with Internet access. The INL provides pre-production testing capabilities (collaborative or independent) in support of current CSO service offerings, including those that must integrate with non-CSO OCIO-sponsored services. The INL enables testing between the INL@MSFC, NASA networks, and the Internet to assist CSO organizations in delivering CSO services. The INL also provides infrastructure services, such as DNS and NTP, providing organizations the ability to remotely design, develop, and stage their solutions in a non-production environment.
3. Network Operations Support Lab (NOSL) – Closed, self-contained environment. The Network Operations Systems Laboratory (NOSL) consists of the same equipment and configurations that are used on production CSO networks. This environment is used to stage systems prior to deployment, replicate problems experienced on production networks and validate root causes and remedies, and optimize implementation procedures.

The CSO SDDL also provides a Network Modeling Service that utilizes virtual computer simulation techniques, including:

- a. Provisioning of the CSO communications environment to evaluate future technologies and systems,
- b. Modeling and simulation techniques to determine changing requirements impacts on the CSO networks, utilizing system engineering methodologies,
- c. Investigation of operational impacts such as cost, technology, support, and performance of new products and services prior to implementation, and
- d. Support for collaboration with engineers, laboratories, and other Federal networks with like interests, to stay current with the trends and evolution of communications technologies.

### 2.14.2 Service Operations

The standard operating hours for SDDL support is 8 am to 5 pm, Monday-Friday, Central Standard Time. Off hours' support can be scheduled in advance. Operations service impacts take precedence over systems engineering/service development and Communications Emerging Technology Working Group (CETWG) activities in the event of resource contention.

If a problem occurs with the SDDL Service, contact the NASA Enterprise Services Desk (ESD) at 1-877-677-2123. The ESD is a 24-hours a day, 7 days a week, 365 days a year organization. Help Desk Analysts create a trouble ticket and dispatch it to the appropriate support organization for resolution.

### 2.14.3 Service Performance

There are no standard performance metrics for this service. Each instance of use is tailored to the project-specific requirements.

### 2.14.4 Service Maintenance

Enterprise SDDL services (Corporate WAN and CETWG) are maintained by CSO and are provisioned as part of the service; however, some services will require Customer funding. Distributed SDDL services are maintained by the host Center.

## 2.15 DTV Support Services

### 2.15.1 General Service Description

Video services for Multi-Channel Digital Television (MCDTV) is a 38.8 Mbps multiplexed video from HQ via the PIP network to a contractor operated teleport for C-band uplink and broadcast to all 50 states. The Live Interactive Media Services (LIMS) is a 12 Mbps video signal from one of 11 NASA centers via the PIP network to a contractor operated teleport for Ku band uplink and broadcast to CONUS. Occasional use remote uplink capability using Ku band broadcast to CONUS is also provided in support of the NASA Office of Communications. The Human Exploration Operations Mission Directorate (HEOMD) Channel is a NASA internal video/audio channel originating from JSC with human space flight mission commentary, live ISS and Russian Space Program feeds. Multiple Live ISS Video Feeds can be received via the CSO PIP Routed data network.

#### 2.15.1.1 Multi-Channel Digital Television (MCDTV)

- 38.8 Mbps, C-band Digital Video Broadcasting – Satellite (DVB-S) modulated uplink from contractor maintained teleport (located in Atlanta, GA.)
- 24x7x365 99.5% availability
- 50 state coverage.
- Three simultaneous uplink programs (NASA Public Channel, NASA Education Channel, and NASA Media Channel).
- MPEG-2 and H.264/MPEG-4 Compression
- NASA owned equipment (routing switchers, video/audio recording equipment, encoders/decoders, multiplexers, ASI switch) is remote controlled from NASA HQ or Goddard TV Operations (Bldg. 28).

- All Video/Audio Encoders located at all 11 NASA centers are controlled locally and remotely at NASA Headquarters and Goddard TV Operations.
- In the event of a PIP Network or related equipment failure (Contingency Mode 1 Failure), either NASA Headquarters or Goddard TV Operations can provide continued uplink programming via direct fiber interface to the Verizon Audio/Video Operations Center (AVOC) in Washington D.C.
- In the event of a loss of NASA Headquarters uplink control capability (Contingency Mode 2 Failure), any of 11 NASA centers can be configured to provide uplink programming with JSC and GSFC configured as prime.

#### **2.15.1.2 Live Interactive Media Service (LIMS)**

- 12Mbps, Ku-band DVB-S modulated uplink from contractor maintained teleport
- Occasional use bandwidth available within 5 day notice for “planned” events and within 24 hour notice for “unplanned” events.
- Purchased on an hourly basis
- 99.5% availability
- CONUS Coverage
- All LIMS services for all NASA centers are scheduled, coordinated, monitored, and cost reconciled by Goddard TV Operations

#### **2.15.1.3 Occasional Use Remote Uplink**

- 12 Mbps, Ku-band DVB-S modulated uplink from remote location via contractor operated flyaway or truck mounted antenna
- Occasional use bandwidth available within 72 hours notice
- Purchased per event on an hourly basis
- CONUS Coverage

#### **2.15.1.4 Human Exploration Operations Mission Directorate Channel (HEOMD)**

- 7.25 Mbps via PIP network
- 24x7x365 availability
- MPEG-2 Compression

#### **2.15.1.5 Live ISS Video Feeds**

- 1.757 Mbps via PIP network
- 24x7x365 availability when authorized
- H.264/MPEG-4 Compression

- Multiple simultaneous live feeds available
- The Communication Service Organization (CSO) provides Six (6) video channels for use by NASA Centers/Projects and **Remote Principal Investigator** (RPI) locations via the Corporate Routed Data network. CSO encodes NTSC video sourced from JSC Building 8, up to 1.5 Mbps per channel using MPEG4/H.264 and distributes in IP multicast or unicast format. JSC Information Systems Directorate (ISD) is responsible for delivery of NTSC video from JSC Building 8 to the JSC NISN PIP demarcation point. Service restoration for ISD resources is <8 hours on weekdays, and on-call on weekends. CSO provides decoding equipment at the HOSC/MSFC TSC, GRC TSC, CSA, GSFC Robotics Lab and the GSFC Space Servicing Center to deliver NTSC video outputs. The RPI sites require the video to be delivered in IP format for viewing on a PC. RPI's are responsible for the transfer of encoded video from the Peering Point to their RPI locations and are responsible for the decoding and display of the received video data delivered in IP format.

#### **2.15.1.6 Verizon AVOC Video Feeds**

- 1.485 Gbps uncompressed HD direct fiber interface
- Direct Duplex HD interface to most Federal buildings (the Whitehouse, Air & Space Museum, State Department, etc. and most domestic and European news media outlets as well as other domestic and European teleport service providers.
- Direct Duplex HD contingency interface to the NASA TV contractor teleport (in Atlanta, Ga.).
- Full remote control of the AVOC switch via Goddard TV Operations or NASA Headquarters.
- Any of 11 NASA centers can be configured to any Verizon AVOC client via Goddard TV Operations or NASA Headquarters control.ISS Video Service transport in support of ISS Operations

### **2.16 Russian Services**

#### **2.16.1 General Service Description**

The Russian Services Group provides a full range of Information Technology support to all NASA projects working within the Russian Federation. The service supports a variety of programs in joint cooperation between the U.S. Government and the Russia Federation, including the International Space Station (ISS) Project. The majority of support is to ISS Real-Time Mission systems and the interchange of data and information between NASA's and Russia's science communities. Support is also provided to the NASA Moscow Liaison Office located within the US Embassy in Moscow.

The current NASA Network infrastructure (Metropolitan Area Network) in Russia consists of Mission and Corporate secure, virtual tunnels and Local Area Networks. The networks support end user Automated Data Processing (ADP) services supporting Real-Time Mission operations

using a converged IP backbone for voice, data and video services. Some of these services are required to sustain and synchronize International Space Station (ISS) activities between the ISS, Russia, Houston and Huntsville Mission Operation systems and facilities. The locations receiving services in the Moscow area for ISS support include: the Volga Apartments, Khrunichev State Research and Production Facility, Moscow Mission Control Center, the Russia Space Corporation - Energia, Gagarin Cosmonaut Training Center, U.S. Embassy in Moscow and the Institute for Biomedical Problems. The locations in Baikonur, Kazakhstan area for Soyuz Packing and Launch support include: Rocket Space Corporation-Energia Area 254 and Hotel 3, plus the Cosmonaut Hotel and Sputnik Hotel. The services in Kazakhstan are highly limited and restricted.

### 2.16.2 Service Operations

If problems occur, In-Country, users will obtain service help by calling the phone number provided to them for this purpose. All other problems should be reported to the NASA Russia Services Group at 1-256-961-4500. After hours phone calls made to this number will rollover to the NISC, which is a 24-hours a day, 7 days a week, 365 days a year organization, and will dispatch the problem to the Russian Services Group.

### 2.16.3 Service Performance

Current service performance parameters for Russia IT Services are shown in Table 8.

*Table 8 Russia IT Services and Performance Standards*

Service	Availability (Percent)	MTTR	Latency (Round Trip)	Other
Mission Critical Voice	99.98	< 5 Minutes	< 700 ms	< 1 percent Harmonic distortion <-40dBm0 noise level Capability to immediately switch to alternate path.
Mission Non-Critical Voice	99.95	< 2 Hours	< 700 ms	< 1 percent Harmonic distortion < -40dBm0 noise level
Admin Voice/Fax	99.95	< 4 Hours	< 300 ms	P3 Grade of Service
Mission Critical Data	99.98	< 1 Minute	< 300 ms	Capability to immediately switch to alternate data path. <.001 percent Packet Loss
Mission Non-Critical Data	99.95	< 2 Hours	< 300 ms	<.001 percent packet loss
Admin Data	99.95	< 4 Hours	< 300 ms	< 1 percent packet loss
Mission/Admin Video	99.95	< 4 Hours	< 300 ms	
Admin Video	99.95	< 4 Hours	< 300 ms	

#### 2.16.4 Service Maintenance

The Russian Services are maintained by CSO and are provisioned as part of the service.

### 2.17 Federal Relay Service

#### 2.17.1 General Service Description

The Federal Relay Service was established by Congress under Public Law 100-542, the Telecommunications Accessibility Act of 1988. The Federal Relay Service provides Relay Operators and Video Interpreters (VI) who act as transparent telecommunication conduits for the transmittal of information through TTY, Videophone, CapTel phone, and Internet browser for individuals with hearing and speech disabilities.

The Federal Relay service enables Federal employees to conduct official duties & broadens employment and advancement opportunities for deaf, hard-of-hearing and speech disabled individuals by ensuring them access to the Federal and Public Telecommunications System. The Federal Relay Service allows the general public (constituents) the ability to conduct business with the Federal government and its agencies. Additionally, The Federal Relay Service enables Federal Government agencies to meet their obligation under Section 504 of The Rehabilitation Act for their employees and constituents with hearing and speech disabilities in workplace and public.

Federal Relay is accessible for both domestic and non-domestic locations. Domestic locations are those within the fifty United States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and the Northern Marianas. All other locations are defined as non-domestic. Certain services of Federal Relay may have geographical restrictions and there are no restrictions on the number, length or type of calls (*i.e. Inbound International via TTY or IP Relay overseas*). All calls are strictly confidential and no records of any conversations are maintained.

The Federal Relay Service contract is for the use of all Federal agencies, authorized Federal contractors, agency-sponsored universities and laboratories; the general public to access Federal agencies; and when authorized by law or regulation, state, local, and tribal governments, and other organizations listed in GSA Order 4800.2E. \_ The Government reserves the right to restrict the use of Federal Relay authorized users as defined above at any time.

#### 2.17.1.1 Service Offerings

##### 2.17.1.1.1 Telephonically-Based Services:

- TTY/Voice/ASCII (a.k.a. TRS)
- Captioned Telephone (CapTel)
- Speech-to-Speech (STS)

##### 2.17.1.1.2 Internet-Based Services

- Video Relay Service (VRS)
- Internet Protocol (IP) Relay

- Relay Conference Captioning (RCC)

### 2.17.2 Service Operation

Traditional Relay Service/TRS (TTY/Voice/ASCII), Speech-To-Speech, IP Relay, and CapTel are available 24/7/365

Video Relay Service (VRS) is available M-F from 7am to 11pm ET excluding Federal Holidays.

Relay Conference Captioning (RCC) is available M-F from 8am to 5pm local time excluding Federal Holidays.

*\* Hours are in reference to English language.*

#### 2.17.2.1 How to request Federal Relay services

- Go to the website: <http://www.fedrcc.us/fedrcc/>.
- Choose “How to schedule a call” for general information
- Choose “Book an event now” to schedule support.
- Fill in the requested information. In the “Federal Agency Name (Required)” drop down, choose “8000 National Aeronautics and Space Administration”
- Notes
  - Required Notice
    - Federal RCC guarantees technical and captioning support for conference calls with 12-hour advance notice. For events with less notice, service cannot guarantee coverage but will attempt to accommodate the request.
  - Canceling a scheduled call
    - Only a limited number of calls per day and each hour can be supported. When the event calendar is full, other RCC call requestors must be turned away. Should your event be changed or canceled, please e-mail the cancellation notice to [cc@captionedtext.com](mailto:cc@captionedtext.com) as soon as possible prior to the scheduled event date and time.

### 3. CSO Local Area Network (LAN) Service

The CSO through the I<sup>3</sup>P contract NICS will provide systems and sustaining engineering for Corporate LAN infrastructure at NASA center locations. The CSO LAN service includes; Corporate LAN, NASA IP Management, Remote Access Service, and Guest Network Service.

### 3.1 Corporate LAN Service

#### 3.1.1 General Service Description

The CSO, through the I<sup>3</sup>P contract NICS, will provide systems and sustaining engineering for Corporate LAN infrastructure at NASA center locations.

This service provides a standard RJ-45 100 or 1000 Megabits per second (Mbps) Local Area Network (LAN) connection to the center's campus network which is typically suitable for desktop computers or printers. The wired LAN connection provides access to the Internet and NASA resources (email, active directory, etc.), although this service does not include accounts to access any resources. Connection speed may be dependent on the center and location.

Service capability and components include:

- Reliable Ethernet wired LAN connectivity
- Compliance with NASA IT Security policies and standards
- 24/7 support via the Enterprise Service Desk

#### 3.1.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

#### 3.1.3 Service Performance

Service Category	Availability (Percent)	Restoral Time	Coverage Period	Latency (Round Trip Time)	Jitter
Corporate LAN	99.90%	TBS	24x7	<10ms	≤5 ms

#### 3.1.4 Service Maintenance

Corporate LAN services are maintained by CSO and are provisioned as part of the service.

### 3.2 NASA LAN IP Management

#### 3.2.1 General Service Description

The CSO, through the I<sup>3</sup>P contract NICS, will provide systems and sustaining engineering to plan, track and manage all NASA Internet Protocol (IP) addresses using NASA IP address management (IPAM) systems and techniques. The NASA CSO IPAM service is defined in detail in section 2.9.5 of this document.

### 3.3 Remote Access Services (RAS)

#### 3.3.1 General Service Description

The CSO, through the I3P contract NICS, will provide systems and sustaining engineering support for the secure remote access systems (e.g. Client Virtual Private Network (VPN), dial-in, Transport Layer Security (TLS) VPN) at each NASA location. This service is typically utilized while working offsite from home or a hotel.

The Remote Access Service (RAS) offers remote connectivity across the public Internet to secure network services and resources. RAS provides authenticated end users who are working away from their offices with secure access to their internal resources and applications. This might include access to files shared on LAN drives, printers and secure applications.

This service is intended to meet the requirements of mobile workers who need to routinely connect to their center network across an unsecured Internet connection. Internet connections may include any unsecured connection such as a Wi-Fi connection at a business or hotel, guest wireless services at another NASA site, a home network, or a cellular data connection.

Service capability and components include:

- Compliance with NASA IT Security policies and standards
- 24/7 support via the Enterprise Service Desk

#### 3.3.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

#### 3.3.3 Service Performance

Service Category	Availability (Percent)	Restoral Time	Coverage Period	Latency (Round Trip Time)
RAS	99.90%	TBS	24x7	NA

#### 3.3.4 Service Maintenance

RAS services are maintained by CSO and are provisioned as part of the service.

### 3.4 Guest Network Services

#### 3.4.1 General Service Description

The CSO, through the I<sup>3</sup>P contract NICS, will provide systems and sustaining engineering in support of NASA Guest Networks at each NASA Center and associated component facility. The Guest Network is intended to facilitate the work of persons who are temporarily located at a NASA

Center or associated component facility, while continuing to protect internal assets (NASA Intranet and Extranet resources).

Guest network services provide temporary network connectivity for users visiting NASA facilities. The network service typically provides Internet access for non-credentialed users. Some centers may also provide other services to credentialed users including email and access to other applications. This service is typically provided over a wireless network although some centers may offer a wired guest network service as well.

Service capability and components include:

- Compliance with NASA IT Security policies and standards
- 24/7 support via the Enterprise Service Desk

**3.4.2 Service Operations**

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

**3.4.3 Service Performance**

Service Category	Availability (Percent)	Restoral Time	Coverage Period	Latency (Round Trip Time)
Guest Network Services	99.90%	TBS	24x7	NA

**3.4.4 Service Maintenance**

Guest Network services are maintained by CSO and are provisioned as part of the service.

**4. Mission Network Services**

The Mission Network Services are divided in two main categories. The first one is the Mission Data Transport Service and the second one is Dedicated Mission Voice Service.

**4.1 Mission - Data Transport Services**

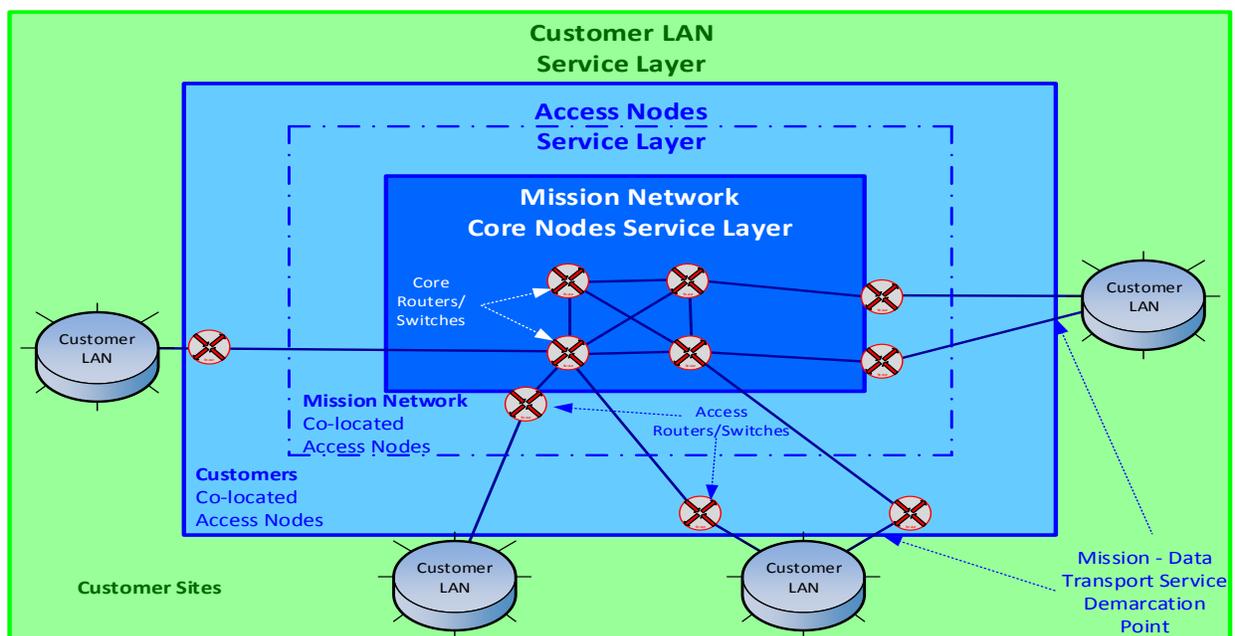
The Mission Network is the infrastructure used to enhance the capabilities needed to offer the Mission Data Transport Services. The Mission Network is built with the capability and the functionality designed to offer data transport services required primarily for and in direct support to the space flight operations. The data transported for space flight operations is typically mission critical and is for telemetry, commands and control, space craft housekeeping, acquisition, tracking and raw science. The Mission Network capabilities have characteristics that differ from traditional IT network capabilities developed to support common infrastructure technology systems. These differences stem from the fact that it is NASA policy (NPD 7120.4D) to design, develop, manage, and operate NASA’s vehicles, system, and assets in a manner which protects the public, astronauts,

pilots NASA workforce, planetary and space environments, high-value equipment and property from harm.

The Mission Network characteristics are defined by its specific network architecture and its unique security policy.

The Mission Network architecture is composed of mission network core nodes and access nodes. The mission network core nodes comprise high-speed switches/routers located at major NASA sites, and are meshed with high data rate circuits. The mission network core nodes are low latency switching/routing elements at the heart of Mission Network. The access nodes are in periphery of mission network and comprise access switches/routers connected to circuits with customized data rate. The access nodes can be located either at NASA sites or customer sites. The access nodes provide data traffic ingress and egress to Mission Network.

#### Mission – Data Transport Service Layers



The Mission Network enforces constraints in addition to the policy stated in Section 1.6.3 of this documents. The use of Mission Network services for normal desktop activities of a Corporate Network – for instance, Internet Service Provider, email, web surfing, social networks, YouTube, and audio streaming – are not permitted on the Mission Network. All acceptable use violations of the Mission Network are submitted as “CAT 4 – improper usage” incidents to the NASA Security Operations Center.

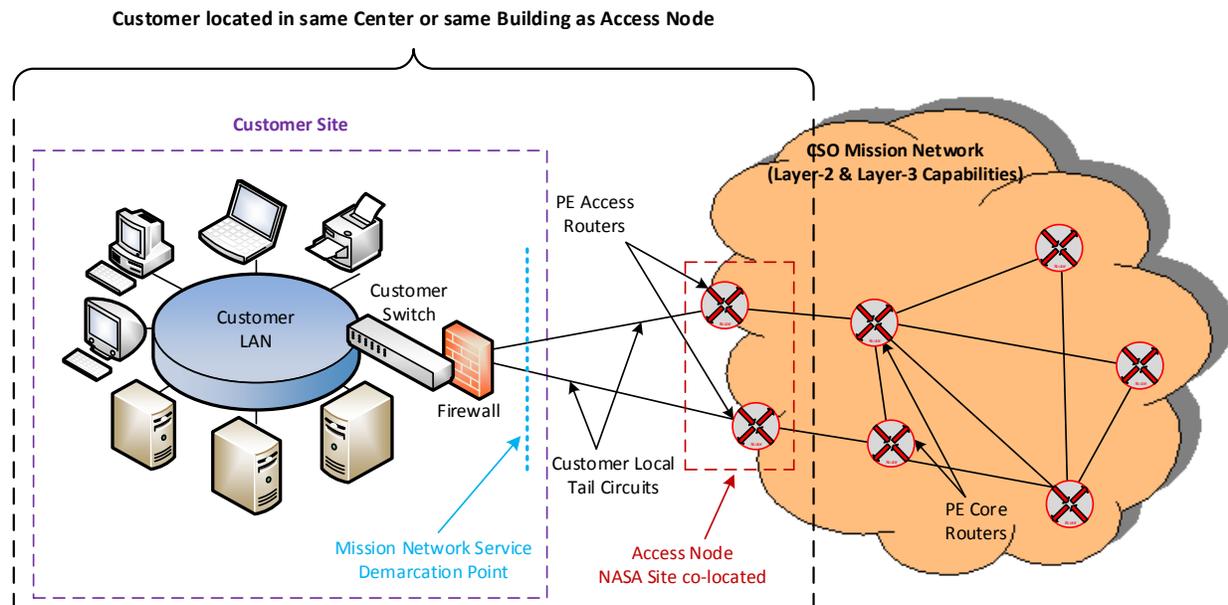
#### 4.1.1 General Service Description

The Mission Data Transport Service offers the option to transport data that originates from a single point to one or several points of destination, with availability and integrity. Typically, the Mission Network capability that offers this service utilizes MPLS, VPN Layer-2 and VPN Layer-3 (from the ISO 7-Layer reference model) to provide a robust architecture capable of supporting a multitude of CSO customers and their diverse mission and security requirements. The Mission

Network capability allows CSO to isolate and transport Project data across a common infrastructure while maintaining the integrity of Projects' security postures. Mission Data Transport Service supports CSO customer and project requirements by offering project specific solutions using Mission Network capabilities and security domains.

The access nodes serve as the points of data ingress/egress to Mission Network and at these points all mission network capabilities are available to provide Data Transport Service to CSO customers either located within a NASA site or customer site outside NASA facility.

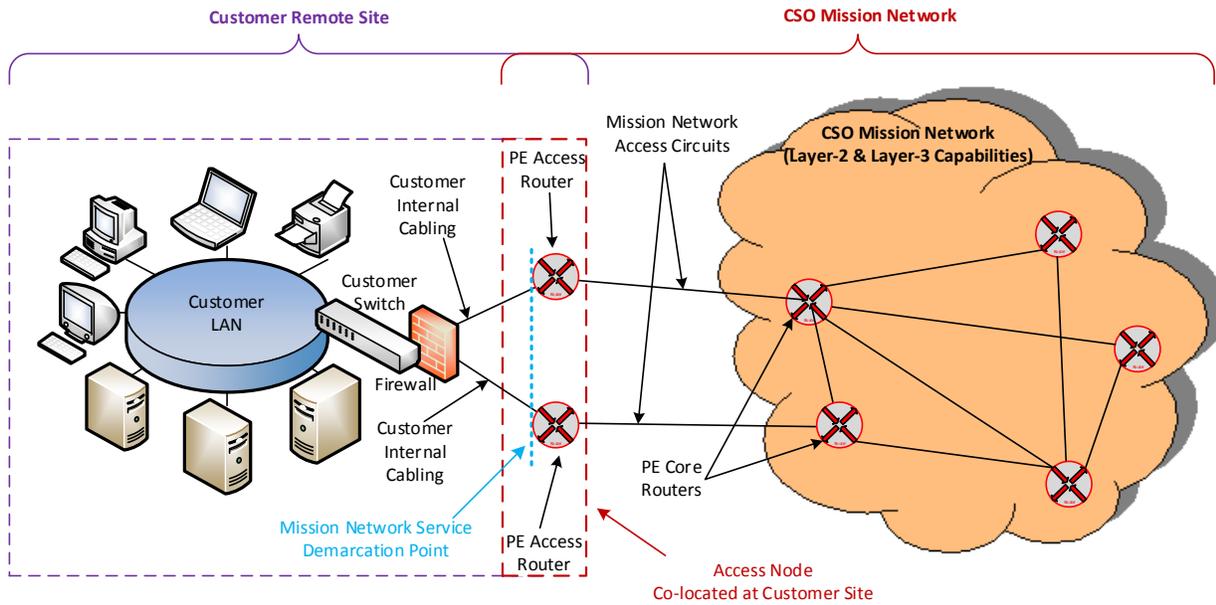
In the case where the CSO customer is located within a NASA facility, a local tail circuit will connect the customer LAN equipment to the access node. If diversity is needed, a second diverse route circuit will be installed.



When the CSO customer site is not within a NASA facility, there are two possible ways to extend the Data Transport Service to the customer LAN and it depends on the network solution that best fulfill the customer requirements.

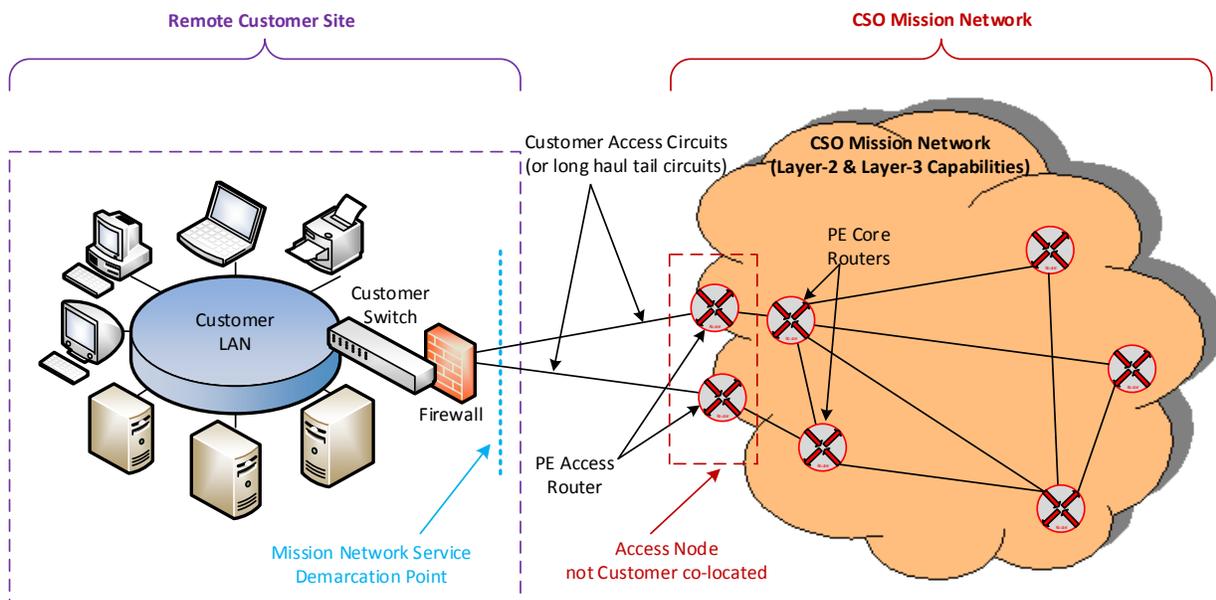
One alternative is to install an access node at the CSO customer premises and directly connect the customer LAN equipment to the collocated mission network switch/router. The access node will connect back to two different (physically and geographically) mission network core nodes with two different circuits offering route diversity. The data rate will be customized to fulfill the requirements provided by the customer.

**Access Node co-located at Customer Remote Site**



Alternatively, if the network solution, to address the CSO customer requirements, does not call for the installation of a co-located access node within the customer premises, a long haul tail circuit will be installed. This circuit will provide the necessary connectivity between the customer LAN equipment and the most appropriate access node selected. If diversity is needed, a second circuit will be installed to fulfill the diversity requirement.

**Access Node not co-located at Remote Customer Site**



The Mission Data Transport Service provides the ground communications for NASA's Human and Robotic Spacecraft, connecting the Mission Operations Control Centers (MOCCS) with the tracking stations. High availability service levels must be maintained to meet Mission-critical spaceflight operations requirements. Administrative data is not transported through the Mission Network. In addition to redundant hardware within the mission network nodes at most locations and diverse circuit routing, Mission Network uses dynamic routing protocols to provide automatic failover for mission real time critical and mission critical service performance. There are some remote customer sites that may require manual intervention for fail over where automatic fail over is not available.

The Mission Network is divided into three logically and physically different security segment: Closed Segment, the intermediate Restricted Segment, and the less restricted Open Segment. Users are audited to maintain the integrity and configuration control of the network.

#### **4.1.2 Legacy Mission Routed Data Services**

#### **4.1.3 Mission Network Security Policy**

Access to and from the Internet and other NASA IP services is extremely limited and provided on a strictly managed "by exception" basis. Further information is found on section 4.1.2.8 "Legacy Mission Routed Data Transport Service – Security Suite.

#### **4.1.4 Service Demarcation Points**

The Service Demarcation Point for CSO Legacy Routed Data Services shall be the Local Area Network (LAN) interface of the CSO Mission router. The LAN interfaces are Ethernet.

Legacy Mission Routed Data Service shall be demarked on CSO owned and controlled switches and routers, or, when a customer tail circuit is installed, at the CSO Carrier owned and controlled circuit terminating Layer-2 equipment.

#### **4.1.5 Service Performance**

There are two service performance categories for mission legacy mission routed data services:

1. Real Time Critical and
2. Mission Critical.

Some customer mission concepts and requirements, and mission network may dictate the need for custom service performance levels other than the above two service performance categories. Both categories support space flight Mission telemetry and other critical data flows. It is noted that these categories influence the capability, architecture and design specifications of the Mission Network infrastructure.

#### **4.1.6 Real Time Critical Service Performance**

This service performance is supported with mission network capabilities using Internet Protocol suite, and it provides a real time critical level to meet the mission requirements associated with the transport of real time telemetry data and other such critical data flows. The Mission Network capabilities supporting Real-Time Critical performance in that it is engineered with a higher level

of redundancy and diversity. This Real-Time Critical service performance allows CSO to achieve a level of availability of 99.98% and benefits from higher priority for problem resolution (restoral time < 1 min). The mission network capabilities supporting this level of service performance employs the same security and connectivity features and limitations as the mission network capabilities supporting Mission Critical service performance.

**4.1.7 Mission Critical Service Performance**

Mission Critical service performance offers a lower level of availability (e.g. 99.95%) and higher period of time for restoral.

**4.1.8 Operations / Trouble Reporting**

If an issue occurs with the legacy mission routed data service, for either mission real-time critical or mission critical service performance, please contact the CSO Communications Managers (Comm Manager) at 301-286-6141 or via Dedicated Mission Voice loops. The Comm Manager is available 24 hours a day, 7 days a week, and 365 days a year. The Comm Manager will work with the appropriate support organization to resolve service operation and performance concerns.

**4.1.9 Service Performance**

The service performance specifications in Table 9 are stated from CSO Service Demarcation Points. CSO cannot guarantee performance beyond CSO’s connections to the Internet or beyond the point of demarcation between Mission Network and the Customer LAN equipment.

*Table 9 Performance Standards for IP Routed Data (by Service Category)*

Service Category	Availability <sup>+</sup> (Percent)	Restoral Time <sup>→</sup>	Coverage Period	Acceptable Packet Loss (Percent)	Round Trip Time <sup>♦</sup>	Maximum Transmission Unit (MTU) Settings (Bytes)
<b>Real Time Critical</b>	99.98	< 1 min <sup>□</sup>	24X7	0.001	<120 ms (CONUS)	1500*
<b>Mission Critical</b>	99.95-99.90	2 hr-4hr <sup>→</sup>	24X7	0.001	<120 ms (CONUS)	1500*

<sup>+</sup> These values apply only for those parts of the Mission Communication service supported by the CSO mission services backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

<sup>♦</sup> Round Trip Time (latency) is specified for data flow between domestic Mission Communications nodes controlled and operated by CSO. Latency is a function of distance and carrier capabilities. User applications that are sensitive to latency shall be engineered to account for the upper limit round trip times specified in the above table.

<sup>□</sup> A capability for immediately switching to an alternate data path shall exist.

<sup>→</sup>This restoral time represents the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.

\*jumbo frames of up to 9,000 bytes can be supported at some locations.

Service Category	Availability <sup>+</sup> (Percent)	Restoral Time <sup>→</sup>	Coverage Period	Acceptable Packet Loss (Percent)	Round Trip Time <sup>♦</sup>	Maximum Transmission Unit (MTU) Settings (Bytes)
Custom	Project Specified	Project Specified	24x7	0.001	<120ms (CONUS)	1500*

#### 4.1.10 Service Maintenance

The Mission Network capabilities needed to provide Legacy Mission Routed Data Services are maintained by CSO and are provisioned as part of the service.

#### 4.1.11 Mission Network Management

The GSFC Communications Control (GCC) manages the Mission Network infrastructure. The GCC operators and NMS proactively monitor all Mission Network devices including firewalls, routers, hubs, switches. GCC Operators and Engineers also perform real time fault isolation including troubleshooting connectivity and data flow problems with other NASA centers and end customers.

Troubleshooting tools such as SNMP traps, statistics, logs and status reports are collected and sent to the Network Management System where the data is displayed to operators continuously with a prioritized alarm structure. Network Probes and many custom scripts assist the operators and engineers in rapidly isolating network faults to provide real time problem solving.

#### 4.1.12 Legacy Mission Routed Data Transport Service – Security Suite

NASA CSO Office provides a suite of data security within Mission Network capabilities for Legacy Mission Routed Data Transport Service. Route and/or traffic filtering may be implemented to provide restricted access to certain sub-networks as specified by the Customer or the IT Security (ITS) requirements. It is important to note that the CSO views security as a responsibility that is shared with the Customer. CSO works with the Customer to identify potential threats and security services for satisfying Customer needs.

All systems, equipment and facilities which connect to Mission Network and make use of the Legacy Mission Routed Data Services shall comply with the Communications Service Office (CSO) Internet Protocol Operational Network (IONet) Security policy.

#### 4.1.13 Legacy Mission Dedicated Data Service

#### 4.1.14 Specific Service Description

The Legacy Mission Dedicated Data Service is used to supplement the Legacy Mission Routed Data Service. The network solution used to provide the Legacy Mission Dedicated Data Service is a customized assessment based on the specific Customer requirements. The infrastructure used to provide the service is the CSO Mission Network capabilities or private circuits outsourced directly from authorized CSO's Communication Service Providers. Mission Network engineers

will select the best network solution based on the requirements coming from the Customer. The data rate for Legacy Mission Dedicated Data Service varies greatly and the capabilities used to offer the service are based on either TDM technology (Time Division Multiplexing technology) or Ethernet. In the former case, the typical data rate can be as low as a fractional T-1 (56Kbps) all the way up to OC-192 (10Gbps). It is to be noted that in exceptional cases the data rates are extremely low rate between 110bps to 19.2kbps. Those extremely low rates are supporting legacy space missions. In case of capabilities based on Ethernet technology, the access data rates are typically 10Mbps, 100Mbps, 1Gbps and 10Gbps. This latter technology allows also for intermediary transport data rate such as 65Mbps (where the Ethernet access is 100Mbps and it is rate limited to 65Mbps).

The CSO Mission Small Conversion Devices (SCDs) can be provided to support legacy spacecraft data conversion and CCSDS/SLE format conversions. These devices are capable of converting any data input type to one or multiple output types to included UDP/IP, TCI/IP, and serial. Additionally, the SCD supports 4800 bit block formats, synchronized frames (serial and TCP/IP), Raw (unblocked data) and variable frame lengths.

#### 4.1.15 **Service Performance Category**

The Legacy Mission Dedicated Data Service is one of the two Transport Data Services offered by Mission Network, consequently, such as for Legacy Mission Routed Data Services, it is primarily used for space flight Mission Critical applications. The levels of performance are the same as defined for Legacy Mission Routed Data Services:

1. Real Time Critical,
2. Mission Critical, and
3. Custom

Some customer mission concepts and requirements, and mission network may dictate the need for custom service performance levels other than the first two service performance categories. These categories support space flight Mission telemetry and other critical data flows. It is noted that these service performance categories influence the capability, architecture and design specifications of the Mission Network infrastructure and the network solution required to fulfill the service performance needed.

#### 4.1.16 **Legacy Mission Dedicated Data - Real Time Critical**

This level of service performance provides the highest reliability with a minimum number of single points of failure. Diversity Mission Network infrastructure is provided and has the fastest repair service. The Mission Network capabilities supporting Real-Time Critical performance in that it is engineered with a higher level of redundancy and diversity. This Real-Time Critical service performance allows CSO to achieve a level of availability of 99.98% and benefits from higher priority for problem resolution (target restoral time < 1 min).

#### 4.1.17 **Legacy Mission Dedicated Data - Critical**

This level of service performance provides high reliability with redundant support hardware and shall include diverse Mission Network infrastructure. The Mission Critical service performance

offers a lower level of availability (e.g. 99.95%) compared to Real Time Critical and has a higher period of time for restoral.

**4.1.18 Legacy Mission Dedicated Data Service – Custom**

This level of service performance will have a customized availability and restoral time which is specified by Project and based upon their budget, and based also on what Mission Network can achieve working with the constraints from the Communication Service Providers network capabilities and limitations.

The current level of service performance parameters are listed in Table 10.

*Table 10 Performance Standards for Mission Dedicated Data (by Service Category)*

Service Category	Availability <sup>+</sup> (Percent)	Restoral Time <sup>→</sup>	Coverage Period	Acceptable Packet Loss (Percent)	Round Trip Time <sup>♦</sup>	Maximum Transmission Unit (MTU) Settings (Bytes)
<b>Real Time Critical</b>	99.98	< 1 min <sup>□</sup>	24x7	0.001	<120 ms (CONUS)	1500*
<b>Mission Critical</b>	99.95-99.90	2 hr-4hr <sup>→</sup>	24x7	0.001	<120 ms (CONUS)	1500*
<b>Custom</b>	Project Specified	Project Specified	24x7	0.001	<120ms (CONUS)	1500*

**4.1.19 Service Maintenance**

The Mission Network capabilities needed to provide Legacy Mission Dedicated Data Services are maintained by CSO and are provisioned as part of the service.

**4.1.20 Mission Network Management**

The GSFC Communications Control (GCC) manages the Mission Network infrastructure. The GCC operators and NMS proactively monitor all Mission Network devices including firewalls,

---

<sup>+</sup> These values apply only for those parts of the Mission Communication service supported by the CSO mission services backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.

<sup>♦</sup> Round Trip Time (latency) is specified for data flow between domestic Mission Communications nodes controlled and operated by CSO. Latency is a function of distance and carrier capabilities. User applications that are sensitive to latency shall be engineered to account for the upper limit round trip times specified in the above table.

<sup>□</sup> A capability for immediately switching to an alternate data path shall exist. <1min is a target restoral time

<sup>→</sup>This restoral time represents the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.

\*jumbo frames of up to 9,000 bytes can be supported at some locations

routers, hubs, switches. GCC Operators and Engineers also perform real time fault isolation including troubleshooting connectivity and data flow problems with other NASA centers and end customers.

## 4.2 Dedicated Mission Voice Service

### 4.2.1 General Service Description

Dedicated Mission Voice Service is a highly reliable service supporting spacecraft activities including processing, preparation, launch, and ongoing spacecraft operations. Mission Voice service is used in conjunction with CSO mission data services and typically constitutes part of a total network solution provided to a specific Mission customer.

The CSO provided service consists of highly reliable, dedicated voice circuits working in conjunction with a real time 24x7x365 Switching, Conferencing, and Monitor Arrangement (SCAMA) hub located at Goddard Space Flight Center (GSFC). The GSFC system serves as the Wide Area Network hub as well as local GSFC. The GSFC SCAMA is based on a Frequentis USA (FUSA) Mission Operations and Voice Enhancement (MOVE) system. These SCAMA voice loops interconnect the different voice distribution systems that support the diverse Mission control centers within the Agency.

The CSO Dedicated Voice service works as a system with the various NASA Center/Customer voice distribution systems. The CSO service, in combination with NASA Center systems, is scalable to meet all current and near future Mission critical loop distribution requirements.

Dedicated Mission Voice Service may constitute part of a total network solution. Each dedicated Mission Voice service is a customized assessment for an individual Customer requirement. The current infrastructure used to support the Dedicated Mission voice service include the Mission Backbone, Point to Point T-1 leased services, and in some cases Point to Point analog.

Dedicated Mission Voice Services are diversely routed to the extent possible based on customer requires and available infrastructure.

### 4.2.2 Service Operations/Trouble Reporting

GSFC CSO serves as Primary SCAMA hub for WAN and local support for GSFC Projects. Services include:

- a. WAN SCAMA services
- b. Real time SCAMA support
- c. Trouble shooting and fault isolation
- d. Enhanced support coverage during critical spacecraft activities
- e. Incident management
- f. System maintenance
- g. Outage reporting and escalation

- h. Conference recording and playback
- i. Line assignments and management

GSFC CSO Local services in addition to WAN

- a. Keypad provisioning and profile management
- b. Keypad maintenance
- c. Cable and Center infrastructure management
- d. Intercom and ring down service

If a problem occurs with Dedicated Voice Service, contact the CSO Communications Managers (Comm Manager) via dedicated Mission Voice Loops or dialup at 301-286-6141. The Comm Manager is available 24-hours a day, 7 days a week, 365 days a year. The Comm Manager will work with the appropriate support organizations to resolve the problem.

**4.2.3 Service Performance**

Current service performance parameters are listed in Table 11.

*Table 11 Networks and Circuits supporting Dedicated Mission Voice*

<b>Service Category</b>	<b>Availability<sup>+</sup> (Percent)</b>	<b>Restoral Time<sup>+</sup></b>	<b>Coverage Period</b>	<b>Latency (Round Trip Time)<sup>♦</sup></b>
<b>Real Time Critical</b>	99.98	< 5 min	24x7	<500 ms
<b>Mission Critical</b>	99.95	<2 hr	24x7	<500 ms
<b>Leased Point to Point T-1</b>	99.95	<2 hr	24x7	tbs
<b>Leased Point to Point Analog</b>	99.95	<2 hr	24x7	tbs
<b>Leased International Mission Voice OCONUS</b>	99.50	<4 hr	24x7	tbs

**4.2.4 Service Maintenance**

Dedicated Mission Voice Services are maintained by CSO and are provisioned as part of the service.

---

## 5. NICS provided Center and Component Facility Services

Center	Network Services		Telecom Services						
	Network	Firewall	Cable Plant	Radio	Phone/ PBX	Cable TV	Public Address	VOIP	EWS
ARC	x	x	x	x	x	x	x		
AFRC	x	x	x				x	x	
GRC	x	x	x	x	x	x		x	
GSFC/WFF	x	x							
HQ	x	x	x		x (SCIF only)	x	x	x	x
JSC/WSTF	x	x	x		x			x	
KSC/VAFB	x	x			x				
LaRC	x	x	x		x	x		x	
MSFC/NSSTC	x	x	Premise Wiring Only						
MSFC/MAF	x	x							
NSSC	x	x	x						
SSC	x	x							
JPL									

### 5.1 Cable Plant Services

#### 5.1.1 General Service Description

The CSO, through the I<sup>3</sup>P contract NICS, will provide Cable Plant services which include operation, maintenance, engineering, design installation, and sustaining engineering of the copper and fiber optic cable plant. This shall include cable management and support for end-to-end configuration/validation tests to meet operational and institutional requirements.

#### 5.1.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

### 5.1.3 Service Performance

Service Category	Return to Service/MAC	Coverage Period	Latency (Round Trip Time)
Outside Cable Plant	3 Business days	NA	NA
Inside Cable Plant	1 Business day	NA	NA
Inside Cable Plant MAC	3 Business days	M-F 6am – 6pm local time	NA

### 5.1.4 Service Maintenance

Cable Plant services are maintained by CSO and are provisioned as part of the service.

## 5.2 Emergency Warning System

### 5.2.1 General Service Description

The CSO, through the I<sup>3</sup>P contract NICS, will provide and maintain the Emergency Warning System (EWS). Emergency Warning Systems support shall be provided for disaster/emergency situations such as fire, explosion, accident, bomb threat, civil disturbance, terrorist-related incidents, and weather related emergencies. Additionally, implementation of emergency warning system service requests and trouble ticket resolution will be performed.

### 5.2.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

### 5.2.3 Service Performance

Service Category	Availability (Percent)	Restoral Time	Coverage Period	Latency (Round Trip Time)
EWS	99.7%	TBS	24X7	NA

### 5.2.4 Service Maintenance

EWS services are maintained by CSO and are provisioned as part of the service.

### 5.3 Public Address System

#### 5.3.1 General Service Description

CSO through the I<sup>3</sup>P contract NICS will operate and maintain the Public Address System. This includes the public address system service requests and trouble ticket resolution.

#### 5.3.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

#### 5.3.3 Service Performance

Service Category	Availability (Percent)	Restoral Time	Coverage Period	Latency (Round Trip Time)
PAS	99.70%	NA	24X7	NA

#### 5.3.4 Service Maintenance

Public Address System services are maintained by CSO and are provisioned as part of the service.

### 5.4 Radio Services

#### 5.4.1 General Service Description

CSO, through the I<sup>3</sup>P contract NICS, will provide radio services required to meet Customer requirements. These services include maintenance of existing capabilities, as well as the development or acquisition, and implementation of enhancements.

#### 5.4.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

#### 5.4.3 Service Performance

Service Category	Mean time to Repair	Coverage Period	Latency (Round Trip Time)
Radio Services	2 Business days	M-F 6am – 6pm local time	NA

#### 5.4.4 Service Maintenance

Radio services are maintained by CSO and are provisioned as part of the service.

### 5.5 Telephone Services

#### 5.5.1 General Service Description

CSO, through the I<sup>3</sup>P contract NICS, will provide the design, installation, operations, maintenance, and sustaining engineering for the telephone system. This will include the implementation of telephone service requests and incident resolution.

#### 5.5.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

#### 5.5.3 Service Performance

Service Category	Availability (Percent)	Return to Service/MAC	Coverage Period	Latency (Round Trip Time)
Telephone Services	99.90%	4 hours	24x7	NA
Handset	NA	8 business hours	M-F 6am – 6pm local time	NA
Handset MAC	NA	3 business days	M-F 6am – 6pm local time	NA

#### 5.5.4 Service Maintenance

Telephone services are maintained by CSO and are provisioned as part of the service.

### 5.6 Voice over Internet Protocol (VoIP)

#### 5.6.1 General Service Description

CSO, through the I<sup>3</sup>P contract NICS, will provide the design, installation, operations, maintenance, system engineering and sustaining engineering for the VoIP system.

#### 5.6.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

### 5.6.3 Service Performance

Service Category	Availability (Percent)	Return to Service/MAC	Coverage Period	Latency (Round Trip Time)
<b>VoIP</b>	99.90%	4 hours	24X7	NA
<b>VoIP Handset</b>	NA	8 business hours	M-F 6am – 6pm local time	NA
<b>VoIP Handset MAC</b>	NA	3 business days	M-F 6am – 6pm local time	NA

### 5.6.4 Service Maintenance

VoIP services are maintained by CSO and are provisioned as part of the service.

## 5.7 Cable Television Services

### 5.7.1 General Service Description

CSO, through the I<sup>3</sup>P contract, NICS, will operate, maintain, and perform sustaining engineering on the cable television distribution system. The contractor shall implement cable television (CATV) service requests and perform trouble ticket resolution within the bands delineated below, and within the estimated/target cost of the contract.

### 5.7.2 Service Operations

If an incident occurs with this service, contact the NASA Enterprise Service Desk at 1-877-677-2123 or by email at [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov). Additional information concerning the ESD can be obtained at <https://esd.nasa.gov>. The ESD is operated 24-hours a day, 7 days a week, and 365 days a year. Help Desk Analysts create an incident ticket and dispatch it to NASA I<sup>3</sup>P Tier II resource.

### 5.7.3 Service Performance

Service Category	Availability (Percent)	Restoral Time/MAC	Coverage Period	Latency (Round Trip Time)
<b>Cable Television</b>	99.7%	8 business hours	M-F 6am – 6pm local time	NA
<b>Cable Television Display</b>	NA	8 business hours	M-F 6am – 6pm local time	NA
<b>Cable Television Display MAC</b>	NA	3 business days	M-F 6am – 6pm local time	NA

### 5.7.4 Service Maintenance

Cable Television services are maintained by CSO and are provisioned as part of the service

## 6. How to Request Services

### 6.1 General

Customers can request CSO services either by contacting the Center/Program representative, Customer Service Representative (CSR) or Mission Services Manager (MSM). Additionally, a Customer can go directly to the Enterprise Service Desk (ESD).

Requests for CSO services shall be submitted to CSO regardless of whether the requirement already appears in a higher level document such as a human space flight Program Requirements Document (PRD), Mission Requirements Request (MRR), and Detailed Mission Requirements (DMR) documents used for non-human flight Mission requirements or Project Service Level Agreement (PSLA) used for Mission and Corporate Network requirements.

### 6.2 The Requirements Process

#### 6.2.1 Customer Actions

Customers initiate contact with CSO by one of the following methods to make known any new service requirements:

- a. Contact your CSO Subject Matter Expert (SME), CSR or MSM (see Appendix C for a list of CSO representatives). This person can do one of two things on your behalf: (1) provide you with complete POC information for dealing directly with the NICS/CSO/Customer Service Representative (CSR) who shall be managing the processing and implementation of your requirement or (2) submit a SR form directly to the NICS/CSO/CSR staff person on your behalf. In either event you shall need to provide all the information necessary for completion of the Service Request form.
- b. ROM Costs and/or Detailed Cost Estimates can be requested via telephone and/or E-mail to your CSR. The points of contact for requesting circuit Rough Order of Magnitude (ROM) Costs and Detailed Cost Estimates are provided in Appendix C. The CSR will generate a SR for the requested ROM or Cost Estimate.
- c. WAN service requests associated with Mission requirements shall be coordinated directly with the CSO Service Owner (SO) (see Appendix C for the name and phone number of the SO responsible for your requirement) or the assigned CSO NICS Customer Service Representative (CSR). The CSO CSR will initiate the required SR process and track the requirement from its receipt to its implementation.
- d. Designated personnel representing existing DCNSS Customers may request adds, modifications, and changes to existing services via the DCNSS Service Request System (SRS). Services – other than routine requests supported by the ESD web site – must be submitted via the standard SR process
- e. As part of the NASA I3P program, NASA established an Enterprise Service Desk (ESD). The service Desk will process requests for all Corporate CSO services. The ESD/ESRS provides Tier 0/1 Help Desk support services in response to reported I<sup>3</sup>P incidents and problems and provides an integrated service ordering capability Enterprise Service Request System (ESRS) for all I<sup>3</sup>P services. The national number and Agency-wide contact information is as follows:

- By Phone: 1-877-677-2123
- By e-mail: [nasa-esd@mail.nasa.gov](mailto:nasa-esd@mail.nasa.gov)
- On the Web: <https://esd.nasa.gov>

## 6.2.2 NASA Communications Service Office (CSO) Actions

Once a request has been received by the CSR, a service request is submitted and undergoes an in-house evaluation to determine the level of service being requested. Part of this validation process includes ascertaining the requirement's validity and that Customer funding will be provided for the requested service, if required.

## 6.3 Rough Order of Magnitude (ROM) Costs and Detailed Cost Estimates

Customers frequently need estimates of what their new communications service requirements are going to cost. Sometimes a very general, rough order of magnitude number may satisfy this need. At other times, the need may be for a fairly accurate estimate of all the costs associated with a set of requirements. CSO shall provide ROM costs and Cost Estimates upon request.

### 6.3.1 Detailed Cost Estimate vs. Rough Order of Magnitude (ROM) Cost

The distinctions between a ROM Cost and a Cost Estimates are described in the following paragraphs:

#### 6.3.2 Rough Order of Magnitude (ROM) Cost

A ROM Cost is a general approximation of the cost of providing a stated service. It is based on experience, costs of similar services, or on a cursory examination of other vendor's rates. A ROM Cost is usually provided to a Customer who is seeking general information. ROM Costs do not include engineering analyses, references to configuration databases, or the development of alternative solutions to generally stated communications requirements. ROM Cost information can normally be provided within 5 working days.

#### 6.3.3 Detailed Cost Estimate

A Detailed Cost Estimate provides a more detailed and comprehensive response than a ROM Cost does. Detailed Cost Estimates are based on the costs associated with a specific solution to a generally stated requirement. Detailed Cost Estimates generally result in dollar figures that include all known cost elements (i.e., labor, additional equipment, overhead, carrier recurring and non-recurring costs, travel (if required), etc.). Given the variability of the factors associated with developing Detailed Cost Estimates, CSO cannot set a general standard that would be applicable to all requests. Often, detailed information is required from sources outside CSO and may only be gained by the issuance of a formal Request for Information (RFI) to industry. However, CSO shall provide the requester with status information and with such cost information (e.g., for those elements of the solution, which have been priced) within 15 working days of receipt of a Request for a Detailed Cost Estimate.

## 7. Communication Services Office (CSO) FUNDING METHODOLOGY

### 7.1 Customer Billing Assumptions FY15 Bill and FY16-FY20 Projected Billing:

- As of October 1, 2012, all funding for CSO services is being managed under the NSSC I3P Working Capital Fund (WCF). For more information on the WCF, please go to <https://nssc.nasa.gov/i3pbo>
- This methodology applies to the following CSO services: Center Local Area Network (LAN) and Security Services, Center Unique Services, Mission and Corporate Wide Area Network (WAN) Routed and Dedicated data, Dedicated Mission Voice, High Rate Data/Video Services, Switched Voice Long Distance Services, Voice Calling Cards, Voice Toll Free services, ISDN for Video Conferencing, Collaboration (Video Teleconferencing Services (ViTS) /Voice Teleconferencing Services (VoTS) and video usage), Mission and Corporate International Services, Desktop Mobile ViTS (DMV) and Data Center and Network Security Services (DCNSS)
- For FY15-FY20 Work Packages (WPs), CSO will apply escalation factors outlined in the NICS contract.
- NICS transformational activities have resulted in Centers sharing costs for Enterprise LAN/WAN Operations and Enterprise Services Software support. Shared costs are provided along with Center Work Package data during the annual PPBE process. Shared costs are currently based upon the number of Center LAN Engineering and Operations Staffing maintained locally (PWS 3.1, 3.3, 3.6) excluding Mission staffing (PWS 3.7 and 3.8) and Center Unique staffing (PWS 4.0)
  - The funding model used to date will be re-evaluated during the upcoming Comm SME F2F.
- For Mission Voice services, the customer will be responsible for funding keysets, facility modifications and costs, and handsets/headsets.
- A “Video Conferencing Usage” charge\* for the ViTS bridging/ops service will be charged to each Center based on the prior year video conferencing usage at that Center. Customers who elected to retain Integrated Services Digital Network (ISDN) services to support their ViTS will be billed for monthly service and usage charges for the ISDN service as well as the ViTS service charges.

- *\*Note on usage charges:* Billing data is collected in minutes for all inbound/outbound ViTS calls. This billing data forms the basis for the Video Conference Usage projection.
- For FY15-FY20, CSO will apply escalation factors outlined by the NASA Headquarters (HQ) Chief Financial Officer (CFO) to customer funded ViTS room refresh estimates. Cost estimates for room refreshes have been updated accordingly in the Customer Project Service Level Agreements (PSLAs). Cost estimates for new room installations are available upon request.
- The initial installation of a Collaboration Facility includes maintenance for all systems in the room up to \$10K per incident for five years. Any replacement of equipment over the \$10K threshold, due to failure, will be funded by the customer. During year four of service, the Customer will be contacted by the CSR to submit a refresh SR in the system. If at the end of the five year period the Customer has not moved forward to refresh (NOT UPGRADE) the room, the room will no longer be under the maintenance policy and supported on a best effort basis.
- The Collaboration rooms are included in the PSLAs. By signing for the PSLA, the requirements owner agrees to “sponsor” that room. We will be contacting room sponsors separately in the near future to discuss ongoing support and anticipated refresh for these rooms; however, for the PSLA, they are simply agreeing to be the sponsor. If the PSLA owner is unwilling to sign up as sponsor, we will remove the room from their PSLA, mark it as orphaned in the PSLA database, and we will schedule the room for decommission.
- CSO is transitioning the new Desktop Mobile ViTS (DMV) service from pilot to production. CSO is targeting an October 1 production date and Center CIOs have agreed to fund this service. Pricing for this will be based on the number of accounts in use at the Center.
- As with any contract, there are costs associated with operating and managing the contract. These allocated costs under NICS include Program Management, centralized tasks, and program fee. The CSO Core funded and Center Work Packages (WPs) will be assessed a portion of these costs based on their usage of the contract.
  - The fixed amount allocation is determined during the spend plan process. This will allow the Centers to plan to a set figure for allocation which should not change except in the case of significant scope increases and/or decreases. Allocation true-ups are done at mid-year and year-end.

- Each Center is responsible for ordering and funding ACES services for the NICS employees located at the Center.
- True-up reconciliation processes no longer exist due to the NSSC I3P Business Office (I3PBO) work books which allow the Center IT RAs to liquidate funding based on actuals. Any excess funding that is received by the NSSC I3PBO may be available to put toward your next year's requirements. Shortages in funding are requested by the NSSC I3PBO as needed to fund invoice payments.

## 7.2 CSO FY16 Funding Strategy:

### Customer Billing Assumptions for FY16 Bill and FY17-FY21 Projected Billing:

- As of October 1, 2012, all funding for CSO services is being managed under the NSSC I3P Working Capital Fund (WCF). For more information on the WCF, please go to <https://nssc.nasa.gov/i3pbo>
- This methodology applies to the following CSO services: Center Local Area Network (LAN) and Security Services, Center Unique Services, Mission and Corporate Wide Area Network (WAN) Routed and Dedicated data, Dedicated Mission Voice, High Rate Data/Video Services, Switched Voice Long Distance Services, Voice Calling Cards, Voice Toll Free services, ISDN for Video Conferencing, Collaboration (Video Teleconferencing Services (ViTS) /Voice Teleconferencing Services (VoTS) and video usage), Mission and Corporate International Services, Desktop Mobile ViTS (DMV) and Data Center and Network Security Services (DCNSS)
- For FY16-FY21 Work Packages (WPs), CSO will apply escalation factors outlined in the NICS contract.
  -
- NICS transformational activities have resulted in Centers sharing costs for Enterprise LAN/WAN Operations, Enterprise Services Software support and Enterprise Engineering support. Shared costs are provided along with Center Work Package data during the annual PPBE process.
  - 
  - For FY16, shared costs are based upon the number of Center LAN Engineering and Operations Staffing maintained locally (PWS 3.1, 3.3, 3.6) excluding Mission staffing (PWS 3.7 and 3.8) and Center Unique staffing (PWS 4.0)
  -

- For FY17-21, shared costs are based upon device count at each Center, with a weighted approach for PPBE18
- A “Video Conferencing Usage” charge\* for the ViTS bridging/ops service will be charged to each Center based on the prior year video conferencing usage at that Center. Customers who elected to retain Integrated Services Digital Network (ISDN) services to support their ViTS will be billed for monthly service and usage charges for the ISDN service as well as the ViTS service charges.
  - *\*Note on usage charges:* Billing data is collected in minutes for all inbound/outbound ViTS calls. This billing data forms the basis for the Video Conference Usage projection.
- For FY16-FY21, CSO will apply escalation factors outlined by the NASA Headquarters (HQ) Chief Financial Officer (CFO) to customer funded ViTS room refresh estimates. Cost estimates for room refreshes have been updated accordingly in the Customer Project Service Level Agreements (PSLAs). Cost estimates for new room installations are available upon request.
- The initial installation of a Collaboration Facility includes maintenance for all systems in the room up to \$10K per incident for five years. Any replacement of equipment over the \$10K threshold due to failure will be funded by the customer. During year four of service, the Customer will be contacted by the CSR to submit a refresh SR in the system. If at the end of the five year period the Customer has not moved forward to refresh (NOT UPGRADE) the room, the room will no longer be under the maintenance policy and supported on a best effort basis.
- The Collaboration rooms are included in the PSLAs. By approving the PSLA, the requirements owner agrees to “sponsor” that room. We will be contacting room sponsors separately in the near future to discuss ongoing support and anticipated refresh for these rooms; however, for the PSLA, they are simply agreeing to be the sponsor. If the PSLA owner is unwilling to sign up as sponsor, we will remove the room from their PSLA, mark it as orphaned in the PSLA database, and we will schedule the room for decommission.
- Desktop Mobile ViTS (DMV) service pricing will be based on the average number of accounts in use at the Center from the previous year.

- As with any contract, there are costs associated with operating and managing the contract. These allocated costs under NICS include Program Management, centralized tasks, and program fee. The CSO Core funded and Center Work Packages (WPs) will be assessed a portion of these costs based on their usage of the contract.
  - The fixed amount allocation is determined during the spend plan process. This will allow the Centers to plan to a set figure for allocation which should not change except in the case of significant scope increases and/or decreases. Allocation true-ups are done at mid-year and year-end.
- Each Center is responsible for ordering and funding ACES services for the NICS employees located at the Center.
  -
- Excess funding that is received by the NSSC I3P Business Service Office (I3PBSO) may be available to put toward your next year's requirements. Shortages in funding are requested by the NSSC I3PBSO as needed to fund invoice payments.

### **CSO FY16 Funding Strategy:**

#### What you pay for:

Customers will be responsible for funding the following **Forecasted** Requirements:

- All OCONUS except SN, DSN, and NEN
- Switched Voice
- Tail Circuits
- Custom Services
- Data Center Network and Security Services (DCNSS)
- Current and Future ViTS over ISDN monthly cost and usage
- Video Conferencing usage
- Replacement equipment for both Video and Voice Conferencing rooms
- Enterprise Shared Work Packages (Center allocations)
- Center Work Packages (WPs)
  - LANs
  - Center services supported by CSO NICS
- ACES services for NICS employees resident at Center
- Desktop Mobile ViTS (DMV)

Customers will be responsible for funding the following **Unforecasted** Requirements:

- Unforecasted, unfunded requirements, typically performed via Service Requests (SRs)

- For Collaboration Services (ViTS and VoTS)
  - All costs associated with Conferencing system equipment and software
  - All costs associated with expediting implementation of room systems
  - All costs associated with travel for installation personnel who provide support for installation of room systems.
  - Labor costs, via SR, associated with dedicated onsite support of ViTS and VoTS meetings.

How you pay for it:

- Each Center has designated a Center IT Resource Analyst (IT RA) who will be responsible for preparing the Funds Commitment Documents (FCDs) in SAP and submitting the corresponding NSSC Advanced Payment Request Form 76 and/or PRs to the NSSC I3P Business Service Office (I3PBSO) for all communication services. All funds should be provided to the Center IT RA. Direct funds will be provided via FCD/Advance Payment Request Form 76. Reimbursable funding will be submitted via PR to the appropriate I3PBO Contracting Officer.
  - See attached listing of Center IT RAs.
- The NSSC I3P Business Office (I3PBO) plans to utilize an FY funding schedule to communicate monthly funding requirements to the Center IT RA.
  - All Centers will complete an initial funding schedule for the I3PBO PPBE17 data call which is due in May. Updates to this schedule will be provided by the I3PBO as needed for new requirements not included in the original projections.
- This method will be used for all CSO services.

What SCaN funds:

- SCaN will be responsible for funding the following existing services:
  - Requirements that are in the CSO Operating Plan
  - SCaN Network
    - Space Network (SN)
    - Deep Space Network (DSN)
    - Near Earth Network (NEN)
  - Collaboration Services
    - Voice Teleconferencing Service (VoTS) Usage (Instant Meeting Service)
    - Sustaining engineering and labor for all CSO provided Video Teleconferencing Service (ViTS) and Voice Teleconferencing Service (VoTS) rooms
    - Refresh and maintenance support for one ViTS full service room per Center. Refresh and maintenance only provided on ViTS equipment. The room supported will be at the discretion and agreement of the Collaboration Service Manager and the Comm SME at the Center. Centers are responsible for providing suitable room upkeep in regards to HVAC, power, and furniture.

- ACES seats for NICS contractor employees (excluding NICS contractors seats covered by centers).

## Appendix A Supported Interfaces and Protocols

### A.1 General

CSO supports the interfaces and protocols listed below. If your particular requirement does not appear on this list, please contact your CSO Service Manager in the Customer Interface Group or your center's Customer Service Representative to determine if it can be satisfied by a standard service offering or if it requires a custom solution (custom solutions cost more than standard offerings).

### A.2 Interfaces

(CCITT) V.35	Differential Emitter Coupled Logic (D-ECL)	EIA RS-530	Stick and Click Connector (SC), Stick and Twist Connector (ST), Optical
Digital Cross-Connect Level 1 (DSX-1)	Electronic Industries Alliance Recommended Standard 232 (EIA RS-232)	EIA RS-449	Registered Jack (RJ)-xx
DSX-3	EIA RS-422	High Speed Serial Interface (HSSI)	Bayonet Neill-Councilmen (BNC)
IEEE 802.3x			

### A.3 Protocols

Subject to waiver action, the use of IP is required for the transport of data across the CSO. Refer to Applicable Documents for specific protocol standard information and waiver processing instructions.

User Data Protocol/Internet Protocol (UDP/IP)	Border Gateway Protocol (BGP)	Multi-cast Open Shortest Path First (MOSPF)
TransMission Control Protocol (TCP/IP)	4800 Bit Block (4800 BB)	Multi-cast
Multilink Point-to-Point Protocol (MPPP)	Consultative Committee for Space Data Systems (CCSDS)	Voice Over Internet Protocol (VoIP)

## Appendix B CSO Service Planning Timeframes

### B.1 General

Table B-1 is a “guide” to assist Customers in the planning of CSO standard services.

### B.2 Standard Interval Factors

The CSO Service standard intervals can be affected by actions and tasks performed by various entities involved in the process. This can include the vendors, the Customer and the host center location. The Customer’s approval of the design package and funding transfer process will affect the CSO Service Standard Intervals.

Many CSO services depend upon local Center support to provide local fiber/cable and/or facilities work such as power provisioning, core drills, conduit, mounting brackets and carpentry work. CSO provides the technical specifications for implementation of these requirements; however the actual submittals for requesting these services and funding of same lies with the Customer. Failure of the Center to complete local Center support tasks prior to CSO service implementation may impact completion dates.

CSO IT security assessments must be approved prior to physical connection of IT resources.

NOTE:

Standard Intervals are based upon business days and new requirements from Customer.

*Table B-1 CSO Service Planning Timeframes*

Service	Design Phase	Implementation Phase	Total
<b>VIDEO</b>			
<b>Custom VITS</b>	25	80	105
<b>VRA/DVA</b>	25	70	95
<b>VOICE</b>			
<b>Custom VOTS</b>	25	67	92
<b>Switched Voice Service (ISDN BRI,PRI)</b>	11	42	53
<b>Toll Free Numbers</b>	0	20	20
<b>Mission Dedicated Voice</b>	32	64	96
<b>Dedicated Data</b>			

<b>Service</b>	<b>Design Phase</b>	<b>Implementation Phase</b>	<b>Total</b>
<b>Mission Dedicated Data</b>	34	81	115
<b>Dedicated Data</b>	20	77	97
<b>Routed Data</b>			
<b>Mission Routed Data</b>	34	81	115
<b>PIP/SIP Routed Data</b>	20	77	97

Timeframes above are based on Networx services T-1 and below. Circuit speeds above T-1 will require additional provisioning time.

Standard Intervals are based upon business days and new requirements from Customer.

Video Engineering Master Schedule may affect implementation timeframe for Video Services.

## **Appendix C NASA CSO Points of Contact (POC)**

### **C.1 NASA Mission Directorate and Mission Support Offices**

CSO personnel are assigned responsibility for requirements processing and implementation based upon the NASA Mission directorate served by the requirement, as well as on program/project and NASA Center or Facility basis. MSM assignments, by Corporate or Mission Services, are found at; <https://cso.nasa.gov>. Where resources permit, the CSO assigns both a primary and alternate person to be the cognizant MSM for each NASA Center or Facility.

### **C.2 CSO On-site Customer Support**

CSO provides Customer Service Representatives (CSR) who are co-located with the Customer and provide on-site support for CSO services, a listing may be found on the CSO website at ;

<https://cso.nasa.gov/contacts>

### **C.3 About this Document**

Send your comments or questions pertaining to this document to the following E-mail address: [Elizabeth.Sudderth@nasa.gov](mailto:Elizabeth.Sudderth@nasa.gov).

## **Appendix D Key Personnel**

### **D.1 CSO Center/Program Representatives**

Centers and Programs have identified personnel to act as liaison between the Center/Program and CSO. A listing of these representatives and their alternates may be found on the CSO website; <https://cso.nasa.gov>

### **D.2 CSO Service Element Managers (SEM)**

The CSO Service Owners can be found at the following website: <https://cso.nasa.gov>

## Appendix E NAMS Instructions for Access to CSO/NICS SharePoint

### NAMS Instructions for Access to CSO/NICS SharePoint site

The following are general instructions on how to submit a Request for access to CSO/NICS SharePoint via NAMS.

1. Launch NAMS (<https://nams.nasa.gov/>)
2. From the **Your NAMS Requests** screen; **type CSO NICS SharePoint** in the box for **New Request**.

**Your NAMS Requests**

NAMS    New Request        Type: All    Center: All

Request Sponsor: Crip, Mary Jean [change](#)

**Note:** Please change your "Request Sponsor" to your supervisor

3. Under the Title header; click on AGCY CSO NICS SharePoint

**Your NAMS Requests**

NAMS    New Request        Type: All    Center: All

Results (max 50)    [Clear](#)

Title	ID	Description	Type	Center
AGCY CSO NICS SharePoint	227878	CSO/NICS collaboration environment.	IT Asset	MSFC

4. Via the "AGCY CSO NICS Sharepoint" page, scroll down to the **Create Request** section and
  - a. Provide **\*Business Justification** details
  - b. In the **Select Options** dropdown; put a checkmark in the box of the site(s) you want to access. *Note: the selected sites will then appear under **\*Sites** as you select them.*

**\* Sites** 3

CAWG    CREW - Service Ch...    CSO

3 of 65 selected

Filter:      Check all     Uncheck all

- CAWG
- CET Lab
- CREW - Network Engineering Reference Documents
- CREW - Service Change Archive
- CREW - Service Change Documents
- CSO

- c. Select the permission level you are requesting under **\*Access**.

**\* Access** 1

Select

**NOTE:** If you need *READ ONLY* to some sites and *CONTRIBUTOR* to others, you will need to complete separate requests (one selecting sites for View-Read Only and one selecting sites for Contributor)

5. Click **Submit Request** button.

**Once your account is created, you will receive an account completion notification from NAMS**

## Appendix F Abbreviations and Acronyms

3DES	Triple Data Encryption Standard
A&A	Assessment and Accreditation
ADP	Automatic Data Processing
AES	American Encryption Standards (AES)
AOPNS	Activity and Outage Posting and Notification System
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASI	Asynchronous Serial Interface
ASN	Autonomous System Number
BGP	Border Gateway Protocol
BMG	Business Management Group
BRI	Basic Rate Interface
CATV	Cable Television
CCB	Configuration Control Board
CCM	Customer Commitment Manager
CFO	Chief Financial Officer
CIG	Customer Interface Group
CIO	Chief Information Officer
CM	Configuration Management
COMSEC	Communications Security
CONUS	Continental United States
COTS	Commercial-off-the-shelf
CSDM	Center Service Delivery Manager
CSO	Communications Service Office
CSR	Customer Service Representative
CVPN	Corporate Virtual Private Network
DCN	Document Change Notice
DCNSS	Data Center Network and Security Services
AFRC	Armstrong Flight Research Center

DHCP	Dynamic Host Configuration Protocol
DMR	Detailed Mission Requirements
DNS	Domain Name Service
DMZ	Demilitarized Zone
DSN	Deep Space Network
DVA	Desktop ViTS Appliance
DVD	Digital Video Disk
EA	Enterprise Architecture
EIGRP	Enhanced Interior Gateway Routing Protocol
E-mail	Electronic mail
ESD	Enterprise Service Desk
ESRS	Enterprise Service Request System
EWS	Emergency Warning System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTS	Federal Technology Service
FY	Fiscal Year
Gbps	Gigabits per second
GCC	GSFC Communications Control
GigE	Gigabit Ethernet
GN	Ground Network
GPS	Global Positioning Satellite
GSA	General Services Administration
GSFC	Goddard Space Flight Center
HEMOD	Human Exploration Operations Mission Directorate
HPREN	High Performance Research Engineering Network
HQ	Headquarters
HRDS	High Rate Data System
HRDVS	High Rate Data/Video System
HSF	Human Space Flight
HSR	Houston Support Room
I3P	IT Infrastructure Integration Program

ICMP	Internet Control Message Protocol
IONet	Internet Protocol Operational Network
IP	Internet Protocol
IPAC	Intergovernmental Payment and Collections
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISS	International Space Station
IT	Information Technology
ITS	Information Technology Security
ITU	International Teleconferencing Union
IVV	Independent Verification and Validation
JSC	Johnson Space Center
Kbps	kilobits per second
LAN	Local Area Network
LD	Long Distance
LIMS	Live Interactive Media Service
MAA	Metropolitan Area Access
Mbps	megabits per second
MCC-M	Mission Control Center – Moscow
MCDTV	Multi-Channel Digital Television
MCIP	Mission Critical IP
MCU	Multipoint Control Unit
MHz	Megahertz
MOA	Memorandum Of Agreement
MONS	Mission Outage Notification System
MPLS	Multi-Protocol Label Switching; Multi-Protocol Lambda Switching
MRR	Mission Requirements Request
MSFC	Marshall Space Flight Center
MSM	Mission Service Manager
MTTR	Mean-Time-to-Restore
NASA	National Aeronautics and Space Administration

NDC	Network Data Center
NEN	Near Earth Network
NESC	NASA Engineering and Safety Center
NISC	NASA Information Services Center
NIIS	NISN Integrated Information System
NISC	NASA Information Support Center
NPD	NASA Policy Directive
NPR	NASA Procedure Requirement
NSAP	Network Service Assurance Plan
NSG	Network Services Group
NSM	CSO Service Manager
NSR	CSO Services Request
NSRS	CSO Services Request System
NSSC	NASA Shared Services Center
NTC	NASA Teleconferencing Center
NTP	Network Timing Protocol
OC	Optical Carrier
OCIO	Office of the Chief Information Officer
OCONUS	Outside Continental United States
ORD	Organization Responsibility Document
OSPF	Open Shortest Path First
PBX	Private Branch Exchange
PING	Packet Inter-Network Groper
PIP	Premium IP
POC	Point of Contact
POS	Packet over Sonet
PPBE	Planning, Programming, Budget, and Execution
PRD	Program Requirements Document
PRI	Primary Rate Interface
PSLA	Project Service Level Agreement
QoS	Quality of Service
RCIP	Real Time Critical IP

RFI	Request for Information
RIP	Routing Information Protocol
ROM	Rough Order of Magnitude
RR	Resource Record
SAP	Service Access Point
SCANS	Space Communications And Navigation Systems
SDD	Secure Data Devices
SDP	Service Delivery Point
SE	Service Executive
SEM	Service Element Manager
SIP	Standard IP
SLA	Service Level Agreement
SME	Subject Matter Expert
SN	Space Network
SOC	Security Operations Center
SOP	Standard Operating Procedure
SR	Service Request
SRS	Service Request System (for DCNSS)
SSL	Secure Sockets Layer
SVS	Switched Voice Service(s)
TLS	Transport Layer Security
UDP	User Datagram Protocol
VBS	Video Bridging Service
VCR	Video Cassette Recorder
ViTS	Video Teleconferencing System
VoIP	Voice over Internet Protocol
VoTS	Voice Teleconferencing System
VPN	Virtual Private Network
VRA	VITS Roll-About
WAN	Wide Area Network
WCS	Web Conferencing Service
WFF	Wallops Flight Facility

WSC

White Sands Complex

## Appendix G Glossary

Availability	A measure of equipment, system, or network performance, usually expressed in percent; the ratio of operating time to the sum of operating time plus downtime.
Bandwidth	A quantified description of the information-carrying capacity of a communications path or link. It can apply to telephone or network wiring as well as system buses, radio frequency signals, and monitors. Bandwidth is measured in (1) cycles per second, or Hz, which is the difference between the lowest and highest frequencies transmitted or (2) in terms of data bits or data bytes per second.
Circuit-switched	A voice or data oriented switched service arrangement that initiates a switched connection on a message or voice call basis.
Closed network	There is neither access to nor from the Internet. Communications are limited to a defined set of authorized addresses.
Core	The service is centrally funded by the OCIO office of NASA HQ.
Customer	A Customer is any organizational entity which validates a network requirement and either directly funds or arranges funding for the requirement. Examples of Customers are officials in NASA Mission Directorates, Mission Support Offices, Program Offices, as well as, Directors of NASA Centers and Field Installations.
Dedicated Services	Services in which communications resources are permanently assigned to one user.
Denial of Service	When a conference cannot be accommodated at the requested time with all requested participants at the originally requested time due to insufficient transmission or bridging capabilities.
E-mail	Basic e-mail service aimed at providing the most basic end-to-end capabilities commercially available. Enhanced electronic mail service has functionality beyond that provided under a basic E-mail offering (e.g., supports electronic commerce requirements, signature authentication, direct fax transfer, group ware support, security features).
E-1	2.048 megabits per second
Filtering	The process of discarding packets that do not meet the network's criteria for forwarding.
Firewall	A firewall is either the program or the computer it runs on, usually an Internet gateway server that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet shall want a firewall to prevent outsiders

	from accessing its own private data resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. Another is to not allow Telnet access into your network (although you may permit your own users to request Telnet connections outside your network).
Grade of Service	The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction. As an example, a P.03 grade of service means there is a 3 percent probability of a call being blocked on the first attempt. The call may go through on any subsequent attempt.
Hyperlink	An element in an electronic document that links to another place in the same document or to an entirely different document. Typically, you click on the hyperlink to follow the link.
Impacted Conference	Any failure that denies a user one or more of the requested functionalities from the room or the network
Intrusion Detection System	Provides real time monitoring of all IP traffic that traverses the perimeter of the network, both inbound and outbound. Inspects all services, protocols, and packets looking for unique attack signatures and shall alert the proper personnel of an attempted intrusion, as well as blocking the IP address, port, and/or service of source system in question
Latency	The time it takes for a data packet to move across a network connection.
Restricted Network	Access to the Internet is permitted but access from the Internet is strictly controlled.
Special Staff	Employees with expert skills in a narrowly defined area, e.g., information technology security. Employees assigned to special staff functions are made available on an as-needed basis, performing duties in support of other organizations when not engaged by CSO.
Switched	Services in which communications resources are shared among many users using a switching device.
Trojan	A Trojan, also “Trojan Horse,” is a program that does something undocumented that the programmer intended, but that some users would not approve of if they knew about it. Some consider that a virus is a particular case of a Trojan Horse, namely one that is able to spread to other programs (i.e., it turns them into Trojans too). Others consider that a virus that does not do any deliberate damage (other than merely replicating) is not a Trojan. Finally, many use the term “Trojan” to refer only to “non-replicating” malware, in which instance the set of Trojans and the set of viruses are disjointed.
Tail Circuit	The circuit extension between the CSO Backbone and the CSO service demarcation at the Customer location. A tail circuit is typically Customer funded.

T-1	1.544 megabits per second
Unit of Service	The standard quantification, sometimes expressed in relation to time, in which a particular WAN service may be priced, ordered, and delivered. A significant deviation from these standard quantifications may result in a tailored (custom) WAN service requirement that in turn shall cause development of a SCANS WAN price quote.
User	The organizational element that is the direct recipient of a CSO provided service, i.e., has one or more physical interfaces used for terminating or originating a CSO telecommunications (see also “Customer”).
Validation	The authentication and confirmation by CSO of a requirement to include an implicit promise of providing such funds as may be necessary to defray the costs incurred in meeting the requirement.
Virus	A computer virus is defined by Symantec as being a parasitic program written intentionally to enter a computer without the user’s permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some viruses do little but replicate, others can cause serious damage or affect program and system performance. A virus should never be assumed harmless and left on a system.
Worm	A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections).

## **Appendix H NASA CSO IT Security Check Lists**

### **G1. Security Check Lists Overview**

New users or services must complete a NASA IT Security Checklist to connect to the IP networks. The specific checklists are tailored to reflect the risks but as a general rule, the following areas must be addressed:

- 1) Personnel - making sure they are trained and have a need for access
- 2) Equipment - dealing with outages, physical security and firewalls
- 3) Software - vulnerability scanning and software updates
- 4) Threat response - processes for dealing with problems
- 5) Ongoing Authorization (annually)

### **G2. The End User Security Assessment Form**

The End User Security Assessment Form checklist is utilized for Corporate network connections (tailsite) external to NASA Centers and can be found at;

<https://cso.nasa.gov/resources/forms>

The completed form is submitted for concurrence to the NASA Center CISO responsible for the program or project that is sponsoring the connection.

### **G3. The Mission Network IONet Security Checklist forms**

**The Mission Network IONet Security forms are utilized for access to Mission IONet data and can be found at.**

<https://cso.nasa.gov/resources/forms>