



Communications Program (CP) Services Document (CSD)

**Version 5
August 2020**

Document Revision Log

Revision	Date	Purpose	Author
1		Performance Parameters Modified	
2		2014 Annual Update	
3		2015 Annual Update	
4		2017 Annual Update	
5		2019 Annual Update	

Approval Authority:

Approval on File

Joseph B. Solomon
NASA Communications Program
Program Manager

August 3, 2020

Date

Concurrence:

Approval on File

Curt Suprock
NASA Communications Program
Deputy Program Manager, Mission

August 4, 2020

Date

Table of Contents

Approval Authority:	2
Concurrence:	3
1. Introduction	7
1.1 Purpose	7
1.2 Scope	8
1.3 Authority	8
1.4 Document Organization	8
1.5 References	9
General Overview	9
2. CP Organization and Functions	9
2.1 Standard Practices	10
2.1.1 General.....	10
2.1.2 Programmatic Goals.....	10
2.1.3 Acceptable Use Policy	11
2.1.4 CP Support Applications.....	13
2.2 Services	15
2.2.1 Planning for Products and Services.....	15
2.2.2 Service Implementation Test and Acceptance.....	16
2.2.3 CP Value-Added Services.....	16
Details	17
3. Corporate Communications Services	17
3.1 Networking Services	18
3.1.1 Wide Area Network Services.....	18
3.1.2 Corporate Routed Data Network	18
3.1.3 Layer 2 Virtual Private Network (L2VPN) Service.....	20
3.1.4 International Services.....	22
3.1.5 Custom Services	22
3.1.6 Network Timing Protocol (NTP) Service.....	23
3.1.7 Enterprise Firewall Services	24
3.1.8 Enterprise Web Content Filter (WCF) Services	24
3.1.9 Network Security Monitoring Services.....	25
3.1.10 DNS, DHCP, and IPAM (DDI).....	25
3.1.11 Corporate LAN Service	28
3.1.12 Remote Access Services (RAS)	29
3.1.13 Data Center Network (DCN).....	30
3.1.14 LabNet.....	31
3.2 Infrastructure/Facility Service	32
3.2.1 Video Teleconferencing Services (ViTS)	32
3.2.2 A/V Conferencing Service Lines	34
3.2.3 Voice Teleconferencing System (VoTS).....	39
3.2.4 Audio Teleconferencing Systems	40
3.2.5 Cable Plant Services	40
3.2.6 Emergency Warning System	41

3.2.7	Public Address System	41
3.3	Collaboration Services.....	41
3.3.1	DeskTop Mobile ViTS (DMV)	41
3.3.2	Instant Meeting.....	42
3.3.3	Internet Protocol TV (IPTV)	43
3.3.4	WebEx	43
3.3.5	Federal Relay Service	46
3.4	Desk Telephone Services	48
3.4.1	Telephone Services	48
3.4.2	Voice over Internet Protocol (VoIP) Service.....	48
3.4.3	Switched Voice Services (including Calling Cards and Toll-Free Services)	49
3.5	Digital and Cable Services.....	49
3.5.1	DTV Support Services	49
3.5.2	Cable Television Services.....	51
3.6	Radio Communications Services	52
3.6.1	Radio Services	52
3.7	Service Operations.....	52
3.7.1	CP Services Management.....	52
3.7.2	MSFC Operations Center.....	52
3.7.3	GSFC Mission Services Operations	53
3.8	Service Maintenance.....	53
4.	CP NASA Communications (NASCOM) Mission Network Services	53
4.1	Overview of the CP NASCOM Mission Network.....	53
4.2	CP NASCOM Mission Network Service Management	54
4.3	Submitting Requirements for CP NASCOM Mission Network Services.....	54
4.4	CP NASCOM Mission Network Services.....	55
4.4.1	CP NASCOM Mission Network Layer-3 Transport.....	56
4.4.2	Layer-3 Transport Embedded Components	56
4.4.3	CP NASCOM Mission Network Layer-2 Transport.....	56
4.4.4	Mission Voice	56
4.5	CP NASCOM Mission Network Ancillary Services.....	57
4.5.1	Installation of Local, Customer Procured “Timing” Devices	57
4.5.2	CP NASCOM Local, Mission Cabling Installation	57
4.5.3	CP NASCOM Mission Network Security Management.....	57
4.5.4	Operations and Maintenance Support.....	57
4.6	Optional Support Provided by NASCOM	58
4.7	Performance Standards for Layer-3 and Layer-2 Data Transport Service	58
5.	Russia Services.....	59
5.1	General Service Description.....	59
5.2	Service Operations.....	59
6.	How to Request CP Services (Corporate and Mission)	60
6.1	General.....	60
6.2	The Requirements Process	60
6.2.1	Customer Actions	60
6.2.2	NASA CP Actions.....	61
6.3	Rough Order of Magnitude (ROM) Costs and Detailed Cost Estimates	61

6.3.1 Detailed Cost Estimate vs. Rough Order of Magnitude (ROM) Cost..... 61

6.3.2 Rough Order of Magnitude (ROM) Cost..... 61

6.3.3 Detailed Cost Estimate 61

7. CP Funding Methodology 62

 7.1 *Customer Billing Guidelines for FY21 Bill and FY22-FY26 Projected Billing:*62

Appendix A. Acronyms..... 69

Appendix B. Definitions 75

Appendix C. Supported Interfaces and Protocols..... 78

Appendix D. CP Services Service Level Agreement (SLA) Measures 79

Appendix E. CP Services Planning Timeframes..... 82

Appendix F. NASA CP Points of Contact (POC)..... 84

Appendix G. Key Personnel 85

Appendix H. NAMS Instructions for Access to CP/NICS SharePoint 86

Appendix I. NASA CP IT Security Check lists..... 87

List of Tables

Table 1: Availability and Service Requirements for DDI Error! Bookmark not defined.

Table 2: Performance Response Times for IPAM Error! Bookmark not defined.

Table 3: Skype Service Performance..... Error! Bookmark not defined.

Table 4: CP Provided Center and Component Facility Services Error! Bookmark not defined.

1. Introduction

Preface

To support the Agency, the Communications Program (CP) provides high-quality, reliable, cost-effective telecommunications systems and services. Customers include all National Aeronautics and Space Administration (NASA) facilities, flight Projects and Programs, as well as national and international partners. CP provides wide area network services to support administrative applications, such as email, general Internet connectivity, access to web-based applications, voice and video conferencing, and collaboration tools that enable the Agency's workforce. CP also provides local services to NASA Centers that include local area networks, voice systems, radio systems, public address systems, emergency notification systems, cable television and cable plant services. The CP provides mission critical data and voice services to connect Flight Projects to Space Communications and Navigation (SCaN) Tracking Networks and other resources, including Space Network (SN), Near Earth Network (NEN), Deep Space Network (DSN), Flight Dynamics Facility (FDF), Launch Complexes and satellite manufacturer and test facilities. CP's Mission services directly support Human Space Flight (HSF) and International Space Station (ISS), including in-country Russia services.

CP collaborates with the other NASA network stakeholders and customers to expedite technology infusion into production networks and services. CP also collaborates with industry to evaluate and analyze commercial hardware and technology that may be useful to NASA. CP collaborates closely with its customers, establishing service level agreements with Projects/Missions and Centers/Facilities regarding service delivery.

The CP strives for transparency and accountability to ensure stakeholder satisfaction and Program success. CP works with other Office of Chief Information Officer (OCIO) stakeholders and with Center Chief Information Officer (CIO) stakeholders to facilitate delivery of CP services to customers. The SCaN and OCIO stakeholders hold primary influence over CP technical and budgetary goals with additional interest by Center CIOs and Communications Subject Matter Experts (SMEs). External partners include International Partners, National Oceanic and Atmospheric Administration (NOAA), Science and Research Partners, Department of Homeland Security, Office of Management and Budget (OMB) and General Services Administration (GSA).

Abstract

This document provides Communications service offerings, descriptions, service performance levels and ordering information for customers.

1.1 Purpose

The CSD provides a single source of services information for CP customers and users. Services are organized into two broad categories, Mission and Corporate. The vision of the CP is to provide to all NASA personnel participating in fulfilling NASA's mission the ability to communicate securely anywhere, at any time, utilizing communications technology that will be so reliable, available, responsive and robust that it will be transparent to the users.

The scope of the CP is the full range of telecommunications and network services and the connection and protection of all network attached endpoints used by NASA, regardless of the location, and the organization providing the service. This includes: Mission, research, and Corporate wide area network (WAN) and local area network (LAN); voice, video and data networking services; and Center (e.g. Facility, Program or Project) unique services (including but not limited to cable plant, emergency warning systems, public address systems, radios, telephones, unified communications, voice over internet protocol, and cable television services).

1.2 Scope

This document encompasses information existing and potential customers may need to request communications services. The requirements submission processes described herein are consistent with and part of the larger processes whereby Mission Directorates, Mission Support Offices, Program Offices, and NASA Centers and Facility installations submit their requirements.

1.3 Authority

N/A

1.4 Document Organization

This document is organized as follows:

- Section 1 contains introductory information.
- Section 2 contains a general overview of the CP organization and functions.
- Section 3-5 contain information on CP's standard commodity and custom service offerings.
 - Section 3 covers Corporate network services
 - Section 4 covers Mission network services
 - Section 5 covers Russia network services
- Section 6 contains information on how one requests services from the CP organization.
- Section 7 contains information on the funding methodology to be used in pricing and charging for services.
- Section 8 contains information on the current funding strategy
- Appendix A contains a list of abbreviations and acronyms.
- Appendix B contains a glossary of terms.
- Appendix C contains information on supported interfaces and protocols.
- Appendix D contains CP services service level agreement (SLA) measures
- Appendix E contains information on CP service planning timeframes.
- Appendix F contains CP POC information.
- Appendix G contains listings of key personnel.
- Appendix H contains NAMS instructions for access to CP/NICS SharePoint
- Appendix I contains a link to the CP security checklists.

1.5 References

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

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.

- NASA Policy Directive (NPD) 2800.1B, Managing Information Technology, expires April 21, 2019 and subsequent revisions.
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2800&s=1B>
- NPD 2810.1E, NASA Information Security Policy, expires June 14, 2020
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2810&s=1E>
- NASA Procedural Requirement (NPR) 2810.1A, Security of Information Technology, expires Dec 16, 2017
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2810&s=1A>
- NPD 2540.1H, Personal Use of Government Office Equipment including Information Technology, expires Feb 24, 2021
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2540&s=1H>
- NPR 2830.1A NASA Enterprise Architecture Procedures, expires Apr 19, 2019
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2830&s=1A>
- CP Standard Operating Procedure CSO-SOP-0002, CP SOP for Trouble Reporting, Activity Scheduling, Mission Freeze and Major Outage Notifications Effective March, 2017
- NPD2190.1B, NASA Export Control Program expires June 20, 2022
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2190&s=1B>
- Federal Information Security Management (FISMA) Act of 2002
 - <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
- NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements Interim Directive 7120.99/NPR7120.7
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=7120&s=7>

General Overview

2. CP Organization and Functions

The Communications Program, under the Office of the CIO (OCIO), maintains an organization responsible for end-to-end service delivery of Program services, projects, initiatives and activities that align with approved Program roadmaps, and operating plans. The CP ensures that Information Technology (IT) investments align with NASA's missions, goals and programmatic priorities while strengthening accountability for IT cost, schedule and performance. The CP includes a business office responsible for financial, budget, contract and customer requirements management.

The CP provides and maintains enterprise and Center-unique services in support of NASA's mission, programmatic and institutional needs, to include:

1. Corporate services delivery
2. Mission services delivery
3. Russia IT services delivery

In order to provide these services, the CP established the NASA Integrated Communications Services (NICS) contract, to provision, operate and maintain enterprise and Center/Facility services as well as assist the CP with requirements-driven, service architecture and service delivery solutions that meet the Agency's communications needs. The NICS contract, a Cost Plus Award Fee/Cost Plus Incentive Fee, 10 year performance-based contract, began in June 2011. In addition to service delivery, the NICS contract provides support of infrastructure projects and services that are uniquely tailored to specific customer communities. This customer-focused approach to service delivery provides customers best of breed, value-driven products and services necessary to meet mission goals, timelines and objectives.

Additionally, the CP holds master agreement/delivery orders under the General Services Administration (GSA) Network contract to provide Corporate and Mission circuits and communications services. The NICS contract provides carrier management support for CP's Network delivery orders to ensure timely delivery of services, appropriate service level targets are ordered and provided and that accurate billing for recurring and non-recurring charges is achieved.

2.1 Standard Practices

2.1.1 General

CP 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.

2.1.2 Programmatic Goals

- Collaborate with other NASA IT Programs, to develop an integrated architecture that improves the End-User experience by standardizing services across all NASA Centers and Facilities.
- Provide effective oversight of OCIO-managed Communications services by developing a common framework for managing, developing, implementing and operating communications services.
- Maintain and enhance an integrated, secure and seamless communications architecture that establishes a secure Agency network perimeter and facilitates a standardized, coordinated, and rapid response to IT security issues.
- Be a trusted NASA IT Communications partner with NASA Centers, Programs and Projects and optimize the communications resources (e.g. architecture, infrastructure, operations and personnel) across the Agency.

- Provide secure solutions that enable seamless collaboration and transparent data sharing across the Agency.

2.1.3 Acceptable Use Policy

The following Acceptable Use Policy, along with the official NASA policy on information technology security and relevant U.S. federal laws, comprises the basic doctrine of the CP.

2.1.3.1 Summary

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

2.1.3.2 Specific

- Use of CP services shall be in support of official NASA Programs. All user requests for CP connectivity shall be validated and supported by a Communications Subject Matter Expert (SME).
- Use of CP resources to support coordination and administrative execution of NASA business is permissible.
- Use of CP resources to support NASA Missions, research, related training and associated technical activities at non-profit institutions of research and education is acceptable.
- Use of CP 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.
- Use of CP 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.
- Use of CP resources to gain unauthorized use of resources attached to the NASA network may result in disconnection and legal prosecution.
- Use of CP resources for the introduction of worms, viruses, Trojans or other software that maliciously interferes with NASA operations is unlawful.
- 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.
- 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.
- Users shall not divulge Internet Protocol (IP) addresses, computer names or any security vulnerabilities associated with a computer system to unauthorized users.
- Users shall not share account(s).
- Users shall not purposely engage in activity with the intent to:
 - Harass other users
 - Degrade the performance of systems
 - Deprive an authorized NASA user of access to a NASA resource
 - Obtain resources beyond those allocated

- Circumvent NASA security measures
- Gain access to a IT resource for which proper authorization has not been given
- Electronic communications facilities (such as social media, electronic mail (e-Mail), 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 CP resources.
- Users shall use the appropriate CP service that meets security and operational requirements of the program data to be transferred.

2.1.3.3 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. CP also utilizes NIST 800-53 recommended security controls for IT systems. CP customers will be required to submit an IT security checklist prior to connection to the NASA network. CP coordinates and manages continuous monitoring efforts to ensure that systems meet Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) and NASA Agency requirements to maintain and or obtain Authorization to Operate (ATO) and incorporate the overall lifecycle of design, acquisition implementation, maintenance, and disposal of architectures, systems, and devices supporting the communications needs of NASA.

2.1.3.4 Information Confidentiality

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

1. A Customer's security level within the CP 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.
2. A Customer's communications access shall be based on the premise that what is not expressly permitted is prohibited.
3. Customer-focused security procedures shall include the reporting and subsequent handling of violations, and accountability for any access controls requested.

2.1.3.5 Internal Safeguards

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

- Sensitivity levels shall be used to minimize the impact of failures in the network
- Customers shall be afforded the least access consistent with their requirements
- Technical controls, such as access lists, packet and content filters, firewalls and intrusion detection/preventions systems shall be employed to ensure that trust is not violated
- Remote access to the network shall be permitted, but only in conformance with policies and practices governing such accesses

- CP shall actively manage firewalls both by technical means and human oversight

2.1.4 CP Support Applications

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

- CSONS: The CSO Notification System (CSONS) is the replacement for the Activity, Outage Plan Notification System (AOPNS) and the Mission Outage Notification System (MONS) Notification systems. CSONS is intended for technical IT staff and is not intended for general users. This tool supports the technical dissemination of notifications related to outages and planned activities. The planned activities are related to the infrastructure/services of CP Corporate, CP Mission, CP Russia and CIO Agency Applications Office (AAO). The outage activities are related to the CP Corporate and CP Mission only. The 'service' based structure of CSONS requires all subscribers to create a NASA Access Management System (NAMS) service based request to receive access to CSONS notifications. To comply with modern identity management policies, the CSONS system does not support email distribution lists (DLs).
 - To register, go to <https://nams.nasa.gov/nams> and search for CSONS. Additional information and Training can be found on the CP Website: <https://cso.nasa.gov/resources/processes-procedures/>.
- iTMS/Call Detail: The Integrated Telecommunications Management System (iTMS) application is a central repository for storing and reporting on various details associated with carrier invoice records including invoice reconciliation and call records for switched voice services. The information is available by month, NASA location, and frequency. The iTMS application replaced the previous Call Detail application.
 - To register, go to <https://nams.nasa.gov/nams> and search for iTMS.

CP Dashboard: The CP Customer Dashboard provides Corporate network device performance (bandwidth, resource usage) for CP Customer access, network device capacity reporting, and Corporate network service status. A Mission events calendar, scheduled activities, and major outage information is provided.

- To register, go to <https://nams.nasa.gov/nams> and search for AGCY CP Dashboard.



- Network Monitoring and Control: The Corporate Enterprise Network Management Systems (CENMS) include event, fault, and performance management applications used by the Corporate Network Operations Center (CNO) that provides seamless, integrated network operations and operations processes capable of managing the CP Corporate end-to-end network services. Center device status and health visibility is available via standard

dashboards and real-time process indicators. Distributed toolsets are available at each Center with central control and consoles at the CNOC. Centralized fault/event/performance management systems include primary and backup core systems at diverse locations utilizing failover and clustering capabilities. The primary CORE system is located at MSFC in Huntsville, AL and the failover CORE is located at Goddard Space Flight Center (GSFC) in Greenbelt, MD. Distributed fault/event/performance management systems are deployed at each Center and used by authorized Center personnel to view faults/events/performance. Also, each Center has available an alternate polling solution should the primary system become unavailable e.g. (scheduled maintenance).

- Access to CENMS applications is restricted to CP and NICS employees only.
- Incident Management: The NICS Information Technology Service Management (NITSM) application provides Mission and Corporate CP/NICS IT service management process support and workflow. This application includes access to incident and problem management, change management, and the configuration management database (CMDB). NITSM is fully integrated to the Tier 0/1 Enterprise Service Desk (ESD) service management tool for Incident and change management escalation to Tier 2 CP/NICS resources. Tickets created at the ESD system are routed to CP/NICS via NITSM for resolution.
 - Access to the NITSM application is restricted to CP and NICS employees only. Customer access to Incidents and change requests should be obtained from ESD directly at <https://esd.nasa.gov>.
- Device configuration management: Provides a vendor agnostic tool to manage the current and historical configurations of all Corporate CP/NICS managed network devices.
 - Capabilities include:
 - Backup and store current network device configurations
 - Restore and rollback to previous configurations
 - Verify changes and compliance
 - Push changes with syntax verification
 - Configuration comparisons of a single device or multiple “like” devices
 - Change notification via email, snmp-trap and/or dashboard
 - Utilizes SNMP, Secure Shell (SSH), syslog and Packet Inter-Network Groper (PING) to interact with devices
 - To register, go to <https://nams.nasa.gov/nams> and search for AGCY CSO Device Configuration

2.2 Services

The NASA CP operates voice, video, and data-based services over on-premise LANs, the NASA WAN, to remote locations and via the Internet, as well as 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 core and Center unique facility services the CP provides Custom services. Custom services are those services that cannot be fulfilled by standard service offerings and typically require additional engineering prior to ordering or providing the service. CP 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 CP 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 CP services entails certain lead times. Appendix E 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.

2.2.1 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 NASA Interim Directive (NID) 7120.7/7120.99, 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

2.2.2 Service Implementation Test and Acceptance

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

- Testing of purchased services such as carrier provided circuits
- Testing of services provided by the existing CP infrastructure supporting Mission and Corporate data, voice, and video services.

When implementing new services, CP 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, CP 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.

2.2.3 CP Value-Added Services

In support of the direct services CP 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 CP 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 (CNOG/Goddard Communications Control (GCC))
- NASA Teleconferencing Center (NTC) Tier II
 - support 0600 – 1800 Central 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)
- Dedicated 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
- NPD2810.1E compliance
- Customer forums
- Property management

- Contract management
- Virtual modeling for conference rooms
- Network integration and consulting
- Transition of applications and protocols to the CP operational network
- Maintenance and operations of CP laboratories
- Interconnection of CP and non-CP laboratories for collaborative research and prototyping
- Development of engineering expertise in emerging systems and technologies
- Coordination with the Agency SOC for 24X7 Intrusion Detection
- Customer training
- Strategy generation and technology innovation

Details

3. Corporate Communications Services

The CP provides and maintains enterprise and center-unique voice, video, and data services in support of NASA's Mission, programmatic and institutional communications needs, to include:

- WAN communications services between all NASA field Centers, NASA Shared Services Center (NSSC), HQ, JPL and to Component Facilities such as Wallops Flight Facility (WFF), Vandenberg Air Force Base (VAFB), GSFC Institute for Space Studies (GISS), and White Sands Test Facility (WSTF)
- Routed data services between NASA Centers, international partners, remote facilities, contractor and research facility locations
- Internet connectivity, IP address management and domain name services, and connectivity to federal research networks, cloud service providers, commercial companies and research institutes
- User-facing communications services
 - Voice over IP
 - Private Branch Exchange (PBX) -based telephony
 - Wired and Wireless LAN services
 - Remote Access Services
 - Unified Communications
 - Voice Conferencing
 - Video Conferencing
 - Video Distribution
- Data center network services in support of Agency and Center data center environments
- Local Center cable plant infrastructure management
- Center-unique services such as Land Mobile Radio (LMR), Cable TV distribution, and emergency notification services

- Center IT security and incident response services, network systems security monitoring and incident management, and enterprise IT security infrastructure management

The CP monitors and manages Corporate network and security infrastructure from its 24x7 Corporate Network Operations Center (CNOOC), located at MSFC. The CP maintains field engineers and technicians at all NASA Centers and remote facilities to support service delivery and maintenance. The Corporate network is managed out of MSFC OCIO organization.

3.1 Networking Services

3.1.1 Wide Area Network Services

The CP backbone is the collection of router hardware, backbone circuits and configuration that provides WAN connectivity between NASA sites. The elements of the Backbone are engineered to provide high capacity, availability, reliability and maintenance levels which ensure that performance exceeds customer SLAs of dependent transported services.

The Layer 2 data service utilizes Multi-Protocol Label Switching (MPLS) based Layer 2 Virtual Private Networks (L2VPNs) configured on the backbone routers. These L2VPNs provide the Layer 2 WAN connectivity, data segregation, traffic engineering and failure recovery for transported services. Any security for transported data is provided by customer connected systems. Encryption is not part of the backbone/layer 2 data service architecture.

The backbone infrastructure topology is a 10 Gigabit Ethernet (10GE) bisected ring passing through 4 core Centers and 3 Carrier Independent Exchange Facilities (CIEF)s. The remaining eleven regional Centers are connected to the ring in two locations at speeds of 10GE or below. The backbone routers are deployed in pairs at all sixteen Centers. Each CIEF only utilizes a single router. Backbone circuits are connected to both Center backbone routers in such a fashion as to ensure a single router outage does not isolate a Center. The Backbone routers at each 10GE core Center are connected to each other via a pair of aggregated 10GE interfaces. Non-core Center Backbone routers are connected to each other via a single Ethernet, equal to or larger than the capacity of the Backbone circuit.

The Backbone infrastructure utilizes high availability and performance routers. These platforms offer redundant core components including route processors, power supplies and switching fabric cards to ensure seamless operation should a single component fail. Each router is capable of 260 Gb per slot and over 400 Gb per slot with upgraded switch fabric cards. Each router is provisioned with 1GE and 10GE interfaces for WAN connectivity and LAN Ethernet interfaces of 100M, 1G and 10G. Additionally it can support 40/100G Ethernet. Efforts have recently been completed to improve latency via topology changes that provide additional paths for traffic to reroute during failure closer to the concentrations of NASA sites.

3.1.2 Corporate Routed Data Network

3.1.2.1 General Service Description

Routed data services include Corporate LAN services in addition to 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 to a remote location from one of the NASA Centers.

3.1.2.2 Routing Protocols

CP 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). CP engineers work with customers to select a protocol consistent with both the Customer's requirement and the enterprise network architecture.

3.1.2.3 Service Demarcation Points

The Demarcation Point (demarc) for CP Routed Data services shall be an 802.3 interface, as defined by the Institute of Electrical and Electronics Engineers (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.

3.1.2.4 Corporate Routed Data Category Descriptions

Two service performance categories for Corporate routed data services have been defined: (1) Premium, and (2) Standard. CP 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 Appendix D. CP SLA Measures.

3.1.2.5 Premium Internet Protocol (PIP) Service (Trust-Side WAN)

PIP service is differentiated from SIP service in that it provides a higher priority for problem resolution, facilities Center to Center communication across the Trust-side WAN and has zero connectivity to the general Internet unless traversing the TIC (Trusted Internet Connection) at one of four locations.

PIP service is most appropriate for internal Agency networking requirements where the Agency's operations should be isolated from the general Internet, traffic flows East-West (Center to Center) or is used as a project specific resource.

3.1.2.6 Standard Internet Protocol (SIP) Service (Untrust-side WAN)

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 prioritization for problem resolution and lower restrictions on acceptable use.

3.1.2.7 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 requirements. It is important to note that CP views security as a responsibility that is shared with the Customer. CP 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.

3.1.2.8 Service Performance

The performance specifications in Appendix D. CP SLA Measures are stated from CP-location to CP-location, (e.g., Center-A to Center-B), and these specifications apply to continental United States (CONUS) connections only. The Customer is also advised that CP cannot guarantee performance beyond CP's connections to the Internet.

For Service Operations, please see [Section 3.7, Service Operations](#).

For Service Maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.1.3 Layer 2 Virtual Private Network (L2VPN) Service

3.1.3.1 General Service Description

The L2VPN Service utilizes an infrastructure that includes a CP-managed backbone service. The L2VPN service is appropriate when the Customer requires transparent extension of LAN services between 2 physical locations. Unlike Corporate VPN service (under Data Center Network (DCN)), L2VPN does not provide data encryption. Use of L2VPN as a solution will be the decision of CP based on established CP and Agency policy. L2VPN service is offered only at established CP backbone services locations.

3.1.3.2 Service Demarcation Points

The demarcation point for the CP L2VPN Service shall be the WAN core router interface of the CP 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.

CP's L2VPN service is independent of the PIP/SIP network service levels. However, the service levels provided meet PIP level agreements. CP 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.

3.1.3.3 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 requirements. It is important to note that CP views security as a responsibility that is shared with the Customer. CP works with the Customer to identify potential threats and solutions for satisfying Customer needs using CP's IT security checklists.

New users or services must complete an End-User Security Assessment Form security checklist to connect to the network.

3.1.3.4 Service Performance

The performance specification in Appendix D. CP SLA Measures is stated from CP-location to CP-location (e.g., Center-A to Center-B) and these specifications apply to CONUS connections only. The Customer is also advised that CP cannot guarantee performance beyond their connections to the Internet.

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.

For Service Operations, please see [Section 3.7 Service Operations](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.1.3.5 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. CP's approach to measuring availability includes the Customer's (demarc) as well as the availability of the shared resources within the network (i.e., the backbone).

3.1.3.6 Restoral Time

CP shall make every effort through its contractors and carriers to restore interrupted service in a timely manner. A requirement has been levied by CP on itself, its contractors and its carriers to return network services to an operational state as indicated in Appendix D. CP SLA Measures.

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 CP 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.

3.1.3.7 Round-Trip-Time

Round Trip Time is measured, monitored, and managed by utilizing Cisco 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.

3.1.4 International Services

3.1.4.1 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, and video.

Expansion of the Corporate Network international services network is accomplished using one or more of the following approaches:

- Sharing CP's backbone circuit extensions with International Partner Agency networks
- Providing CP tail circuit extensions from a NASA site to an International Partner Agency location via a Trusted Internet Connection (TIC) location.
- Establishing research network or general internet peering arrangements
- New users or services must complete a NASA IT security checklist to connect to the CP IP networks.

3.1.4.2 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 CP and its providers to meet those requirements. The best possible SLA guarantees are provided to the Customer when all dependencies have been identified.

For Service Operations, please see [Section 3.7 Service Operations](#).

For Service Maintenance, please see [Section 3.8 Service Maintenance](#).

3.1.5 Custom Services

3.1.5.1 General Service Description

Custom telecommunications 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 CP's Corporate network.

3.1.5.2 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 CP and its providers to meet those requirements. The best possible SLA guarantees are provided to the Customer when all dependencies have been identified.

For Service Operations, please see [Section 3.7 Service Operations](#).

For Service Maintenance, please see [Section 3.8 Service Maintenance](#).

3.1.6 Network Timing Protocol (NTP) Service

3.1.6.1 General Service Description

The NTP is an Internet Protocol that is used to synchronize a computer's clock to a reference time source. The NASA (CP) 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 CP NTP servers respond to host polls with Coordinated Universal Time (UTC) timestamps with no offsets for any time zones. The NASA CP NTP servers provide UTC which is adjusted for leap seconds.

The NASA CP NTP service consists of servers accessible via the PIP networks MSFC, GSFC, ARC, KSC, and JSC. Hosts located on any trusted NASA network may use the service by pointing to one or more of the following:

Location	PIP-B	PIP-A
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 Global Positioning Satellite (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 Active Directory (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 CP source (round-robins the ten NASA servers).

- Public - time.nasa.gov points to ntp.nasa.gov (managed out of ARC 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 CP 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.

3.1.6.2 Service Performance

There are no performance metrics for this service.

For Service Operations, please see [Section 3.7 Service Operations](#).

For Service Maintenance, please see [Section 3.8 Service Maintenance](#).

3.1.7 Enterprise Firewall Services

3.1.7.1 General Service Description

The enterprise firewalls are located at the perimeter of the WAN and are managed by CP/NICS. These firewalls are in support of Agency goals and objectives to enhance mission success by providing efficient and effective access to resources within internal NASA networks, while providing IT Security decision makers the ability to enforce common controls using consistent security policies across the enterprise. The firewalls provide Next Generation Firewall services such as application control and Unified Threat Management solutions. Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) policies for the enterprise firewalls are governed by the CyberSecurity and Privacy Division (CSPD). Changes to the policies should be requested through the Office of Cyber Security Services (OCSS). Once approved the requests are implemented by CP/NICS enterprise services.

3.1.8 Enterprise Web Content Filter (WCF) Services

3.1.8.1 General Service Description

The Enterprise WCF's are part of the Unified Threat Management suite located at the perimeter of the WAN. All HyperText Transfer Protocol (HTTP) traffic traversing the Corporate network for internet access will be scanned by the WCF regardless of source/destination port. HyperText Transfer Protocol Secure (HTTPS) traffic is scanned with certificate inspection. The Enterprise WCF service consists of three main parts: the URL Filter, the category filter, and the content filter. URL filtering acts upon URLs by checking them against a whitelist/blacklist and applying the selected action. Category filtering checks the URL against categories that have been designated by Agency policy for appropriate use. The content filter checks the content of the webpage against words, phrases, or sentences and assigns a score to the webpage that can then be allowed or blocked.

When a user attempts to access a resource that is blocked by policy they will be presented with a block screen to notify them of the action that was taken. The block screen also notifies the user of the URL that was blocked and the category that the URL belongs to. Remediation steps are included on the block screen which allow the user to send an email to their local IT security office

including the URL and category for assessment. If the URL is determined to be mis-categorized or blocked in error, action can be taken to resolve the block.

Policies for the enterprise WCF's are governed by the Agency IT Security organization. Changes to the policies should be requested through the Office of Cyber Security Services (OCSS). Once approved, the requests are implemented by CP/NICS enterprise services.

3.1.9 Network Security Monitoring Services

3.1.9.1 General Service Description

The (SOC), located at the ARC, maintains security monitoring systems that are strategically deployed within CP networks 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.

NASA's SOC is tracking, monitoring and reporting issues 24x7x365. For more information or to report an issue, contact 1-877-NASA-SEC (1-877-627-2732) or soc@nasa.gov.

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

3.1.10 DNS, DHCP, and IPAM (DDI)

3.1.10.1 General Service Description

Through the DDI service, CP provides Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Autonomous System Number (ASN) management and IP address management (IPAM) services for all IP resources assigned to NASA. CP 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. Local network management personnel utilize the CP DDI system (application and data repository) for day-to-day management and monitoring of local IP resources. DDI resource usage must follow the guidelines set forth in the document NITR-2830-1C, Networks Using NASA IP Resources or NASA Physical Space, which can be found on the NASA Communications Architecture Working Group (CAWG) SharePoint site: [IP Addressing - Use Policy](#).

3.1.10.1.1 DNS

CP 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 American Registry for Internet Numbers (ARIN) and DOTGOV. Web service policy is set by the Web Services Office (WSO) of the Agency OCIO, and administered as applicable, by the CP through the DDI service.

Creation of new second-level domains or NASA.GOV-level domain names shall require the approval of CP and Agency (OCIO) management in accordance with Agency and Federal Policies.

3.1.10.1.2 DHCP

CP 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.

3.1.10.1.3 Internet Protocol Address Management (IPAM)

CP provides top-level management of all IP address space and ASN 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). CP may assign NASA IP address space for NASA Customer use for the life of approved NASA projects. CP 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 CP and 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: [IP Addressing - Use Policy](#).

3.1.10.2 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 CSONS.

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 4 servers distributed regionally within a single network hop of any NASA Center. Public (Internet) services are provided with a total of 3 servers aligned with CP Internet Peering Points. Recursion services are provided with a total of 5 caching servers, located at NASA core WAN sites.

Table 1: Availability and Service Requirements for DDI

Item	Explanation	Objective
Wide Area Network service Provided by CP	DDI traverses CP's infrastructure for intra-and extra-Agency services, including the Internet.	Overall availability provided by CP 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 CP	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 DCN infrastructure, and a backup central server located on the GSFC DCN 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 DCN section of this document for performance metrics associated with network connectivity.
Local System Availability (DNS, DHCP) Provided by local network management organization (CP 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.

3.1.10.2.1 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 3.

Table 2: Performance Response Times for IPAM

Transaction	Expected Performance
Intra-Agency DNS lookup	<p>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.</p> <p>Exception: 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.</p>
Extra-Agency DNS lookup	<p>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.</p> <p>Exception: 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.</p>
DNS Record Change Requests	<p>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 (CP or other).</p>

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

For Service Operations, please see [Section 3.7 Service Operations](#).

3.1.11 Corporate LAN Service

3.1.11.1 General Service Description

The CP, through the NICS contract, provides systems and sustaining engineering for Corporate LAN infrastructure across 10 NASA Centers, HQ and component facilities.

This service provides Wired and Wireless LAN connectivity to the Internal, Visitor (Guest) and Specialized (Partner, Lab, Project, etc.) campus networks. Wired services are provided using standard RJ-45 100 or 1000 Megabits per second (Mbps) LAN connections which are typically suitable for desktop computers, printers, VoIP phones, etc. Wireless services are provided using standard 802.11n (theoretical max speed of 450 Mbps) or 802.11ac (theoretical max speed of 1300 Mbps) wireless access points which are typical suitable for laptop computers, smartphones, tablet, etc. Wired and Wireless connections to the Internal LAN provides access to NASA

resources (email, active directory, etc.), and the public Internet. Wired and Wireless connections to the Visitor (Guest) LAN provides limited access to the public Internet. This service is intended to facilitate connectivity for NASA employees' personal devices and the work of temporary, non-credentialed visitors to NASA facilities, while protecting internal assets. This service does not include accounts to access any resources. Wired and Wireless connection speeds may vary per Center and location. The Partner network is an example of a specialized network that provides NASA contractors with a network that allows their Company provided devices to get connectivity back to their company resources. Any access to NASA resources would require an approved remote access method.

Service capability and components include:

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

3.1.11.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, SLA Measures](#).

3.1.12 Remote Access Services (RAS)

3.1.12.1 General Service Description

The CP, through NICS, will provide systems and sustaining engineering support for the secure remote access systems (e.g. Client Virtual Private Network (VPN, 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

3.1.12.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.1.13 Data Center Network (DCN)

3.1.13.1 General Service Description

DCN 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.

- LAN connectivity for agency wide server applications
 - Switch ports (100,1000, 10000Mbps)
 - IP address assignment
 - DNS service
 - Server network-based load balancing
 - Geographic load balancing

- WAN connectivity
 - Direct connection to CP WAN
 - Network-to-Network VPN is provided by to other Centers and partners. This service provides an encrypted tunnel between two networks. CP's Network-to-Network VPN service supports the Advanced Encryption Standard (AES) (AES128, AES192, and AES256). The devices used are Federal Information Processing Standard (FIPS) 140-2 compliant.
 - Client-to-Network VPN tunnels for system administrator access to server resources

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

- Intranet Network – supports Data Center servers for Agency wide services intended for internal NASA use only.
- Public Network – supports Data Center servers for Agency wide services intended to be accessed from the Internet.
- Demilitarized Zone (DMZ) Network – Provides a secure path for traffic flowing between the Intranet and Public Networks and to the CP WAN

3.1.13.2 Service Performance

DCN is maintained by CP 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.

For service operations, please see [Section 3.7, Service Operations](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.1.14 LabNet

3.1.14.1 General Service Description

LabNet data service provides network connectivity to research partners located at sites across the NASA network environment and at research partner facilities. LabNet connectivity is utilized to support research, prototype testing and integration for mission projects prior to progressing to formal acceptance testing. This service is implemented by coordinated efforts across the following service lines; LAN, CP Backbone, Corporate Routed Data, Firewall and Cable Plant. Leveraging of these service lines in the CP provided design is dependent upon the data transport model that is employed to satisfy the requirement.

3.1.14.2 LabNet Sites within a NASA Center or between NASA Centers

Provides data transport to LabNet sites inside a single center's network or across multiple center networks which require the ability to communicate with each other. If all sites exist on a single center's network infrastructure and LAN to LAN encryption is not required, these data sets would flow from the LabNet site at one building to the LAN demarcation point through the access layer of the LAN on a VLAN set aside for LabNet traffic. At the distribution layer the traffic would then be routed to the destination LabNet enclave through a VRF. In this instance, data sets will not leave the center LAN infrastructure.

In the event that LabNet sites at different Centers require encrypted data transport between each other the partner Lab will provide the firewall/router terminating an IPSec tunnel at lab. These data flows would utilize a LabNet VLAN and the LabNet VRF inside the LAN to communicate across the CP backbone via the LabNet L2VPNs established for the service. The IPSec tunnel would terminate on a LabNet VDOM at the Agency Cloud FWs. Data would then be statically routed inside the VDOM to the destination site(s) via another IPSec tunnel. In this instance, the FW VDOM enforces policy either permitting or denying sites to communicate with each other.

3.1.14.3 LabNet Sites To Off-Premise Research Partner Facility

Provides data transport to an on-premise LabNet site(s) requiring communication to an off-premise research partner lab(s). This data flow would utilize the LabNet VLAN/VRF at the center LAN and ingress the WAN via the LabNet L2VPN. The data would be routed to the LabNet VDOM at the WAN DMZ. The data would then traverse the TIC stack unencrypted for inspection prior to ingressing the VPN VDOM on the TIC FW. The traffic would then flow to the remote lab via an encrypted site to site tunnel. In this instance also, the FW VDOM enforces policy either permitting or denying sites to communicate with each other.

3.1.14.4 Service Demarcation Points

The Demarcation Point (demarc) for LabNet services shall be an 802.3 Ethernet interface, as defined by the Institute of Electrical and Electronics Engineers (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.

3.1.14.5 Internet Protocol (IP) Routed Data – Security

LabNet provides security to data flows via segmentation, encryption, route filtering and traffic filtering as needed to provide restricted access to LabNet networks as indicated by Customer or IT security requirements. It is important to note that CP views security as a responsibility that is shared with the Customer. CP works with the Customer to identify potential threats and solutions for satisfying Customer needs.

New users or services must complete a NASA IT security Interconnection Security Agreement (ISA) before connection to the network is permitted. CP Cybersecurity team will work with the LabNet partner to complete the ISA documentation process.

3.1.14.6 Service Performance

The performance specifications in Appendix D. CP SLA Measures are stated from CP-location to CP-location, (e.g., Center-A to Center-B), and these specifications apply to continental United States (CONUS) connections only. The Customer is also advised that CP cannot guarantee performance beyond CP's connections to the Internet although general SLA goals are provided.

For Service Operations, please see [Section 3.7, Service Operations](#).

For Service Maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.2 Infrastructure/Facility Service

3.2.1 Video Teleconferencing Services (ViTS)

CP is responsible for room equipment, operations, and the scheduling of Video Teleconferencing Services, but is not responsible for transport of the data. Physical changes to rooms where systems are provided by the NASA Locations are completed by the facilities organizations at the resident Center. CP A/V Conferencing Services coordinates with the appropriate service organizations to ensure the communications connectivity to the rooms is provided.

3.2.1.1 Service Description

The CP A/V Conferencing Service 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.

CP A/V Conferencing services include engineering, provisioning, installation, and maintenance of Agency wide video-conferencing facilities and the network infrastructure that support the video bridging operations supporting multipoint conferencing.

The NTC, located at MSFC, is responsible for scheduling bridging services, monitoring video bridging operation and collecting usage metrics. 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 CP's NTC scheduling procedures, or to learn more about A/V Conferencing, please refer to the Video Conferencing Home Page at:

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

The NTC 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.

3.2.1.2 ViTS Interface Types

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

3.2.1.3 ViTS Facilities

Video Conferencing Facilities are both Core and Customer funded, and consist of Custom and Standard configurations, to include, though not limited to Desktop, Office Spaces, HuddleSpaces, Multi-Media facilities and full service Conference Rooms. 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 (3) participants to seven participants.



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

3.2.1.4 CP Core Conference Rooms

These are Full-Service Conference Rooms, funded by CP and located at each NASA Center and selected Associated Facilities. The rooms 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.



3.2.2 A/V Conferencing Service Lines

The NASA CSB approved a suite of enterprise agency/enterprise conferencing solutions, based on current requirements, Communications Target Architecture (CTA) and Approved Products List (APL). The standardization of legacy Center-provisioned conference equipment and rooms, roles and responsibilities and agency/enterprise direction are critical in the implementation of the approach.

Enterprise Conference rooms are a standardized and comprehensive set of CP Collaboration service offerings based on CTA and APL. The systems and service lines that are considered conference rooms support multiple participants, video conferencing (point-to-point or multipoint), desktop mobile, multimedia and content sharing as well as integrated and installed (standalone) audio systems. Currently, the systems and service lines that are determined to be outside the CP Enterprise scope are auditoriums, table top audio appliances (PODS) and portable projectors.



3.2.2.1 Installed Audio

This conferencing package is designed to stand alone as a robust audio matrix conferencing system. The system is made up of the highest quality components and delivers consistently clear audio quality.

Collaboration Services Installed Audio is simply the easiest way to add superior quality to any conferencing environment. The familiar interface is both simple and elegant with programmable features that make it powerful as well.



3.2.2.2 OfficeSpace



OfficeSpace is a multimedia conferencing package. This design features an under table computer interface with available wireless content sharing, with video displays. An individual or small group can be sharing ideas within seconds of entering an OfficeSpace.

3.2.2.3 HuddleSpace



The HuddleSpace is a multimedia conferencing package designed for small conference areas that typically seat from 2 to 6 participants. This design features a display with connectivity for a computer or mobile device such as a smartphone or tablet. The HuddleSpace is optimized to support today's latest mobile conferencing devices. The HuddleSpace allows meetings to take place without the setup time involved with larger controlled conferencing systems. A small group can be sharing ideas within seconds of entering a HuddleSpace.

3.2.2.4 HuddleSpace – VTC

The HuddleSpace – VTC is a video conferencing package designed for small conference areas that typically seat from 2 to 12 participants. This design features the Cisco SX80 codec with in a single or dual display configuration. The versatility of the SX80 allows it to be used as an all-in-one video and multimedia conferencing solution which gives the user more control of the conference from a single touch panel interface. The HuddleSpace-VTC allows meetings to take place without the setup time involved with larger controlled conferencing systems. A small group can be sharing ideas across the Agency within seconds of entering a HuddleSpace-VTC.



3.2.2.5 Media One

Media One is a multimedia conferencing package designed for small to medium sized conference rooms that typically seat from 2 to 12 participants. This design features the AMX all-in-one AV switcher and control system with a 7" touch panel. The control system is designed utilizing a user-friendly interface recognizable by all our customers. *The most common scenario in a meeting is for a presenter to show content from a laptop or room PC on a display, and it's simple in the MediaOne conference room. There are no complicated remotes, no switching of sources on the display, and no searching for the right cable. With the MediaOne, it's as simple as pressing an icon.*



3.2.2.6 Media Plus



The Media Plus is a multimedia conferencing package designed for small to medium sized conference rooms that typically seat 15 to 30 participants. This design features the AMX all-in-one AV switcher and control system with a 10" touch panel presenting the recognizable NICS Interface. *Dual displays are the most common customer requirement for content display across the Agency. In the past this meant large and pricy matrix switchers and multiple customized components. The new MediaPlus series fills the gap between the basic*

HuddleSpace and the NICS fully Custom Media room.

3.2.2.7 Media Plus – VTC

Media Plus – VTC is a multimedia and video conferencing package designed for small to medium sized conference rooms that typically seat 15 to 30 participants. This design features the AMX all-in one

AV switcher and control system with a 10" touch panel featuring the recognizable NICS Interface. This system offers an economical yet powerful video conferencing solution for any mid-level corporate environment.



3.2.2.8 Custom Media

With a fully scalable matrix and limitless control, the Custom -MEDIA system is capable of meeting any design requirements from a single display to multiple displays or video walls.

Custom Media is a multimedia conferencing package designed to be customizable for any venue. This design features the AMX DGX AV switcher and control system with a 20" touch panel featuring the recognizable NICS Collaboration Services Interface.



3.2.2.9 Custom VTC

These are typically Full-Service Customer funded Conference Rooms, used for large videoconferences, and multimedia presentations, that can accommodate 30-200 persons. *This offering is the most versatile option for large conference rooms. With a nearly endless array of options and can be adapted to the most exacting requirements, while maintaining standardization across the Agency.* A new Custom Conference Room is designed to the Customer's specification. Custom VTC is a multimedia, audio and video conferencing package designed to be customizable for any venue. Standard capabilities include HD dual flat panel displays and/or projection systems. This design features flat panel displays or Projectors, 20" Touch Panel Control, Video Cameras, Pop-up Tabletop Interfaces, Mutable Table Microphones, Blu-ray Player, Cable Television (CATV) Tuners, Audio Recording, Video Recording, LED Room Status Signs, Wireless Presentation among the options, to include video wall configurations



3.2.2.10 Service Performance

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

- At a minimum, the video Conferencing Bridge Multipoint Control Unit (MCU) shall support up to 20 NASA community locations participating in 1 to 10 simultaneous and independent conferences.
- If endpoints are compatible with AES, the infrastructure can support encrypted video calls.

- The mean time to restore network service for an in-progress conference shall be less than or equal to 4 hours.
- The mean time to restore service for non-conference impacting problems shall be less than 2 business days.
- Conference availability shall be at least 99.5 percent to include room systems, CP provided transport, and multipoint control system.
- IP service shall be provided at the Corporate Premium Routed Data Service Level.

The use of CP A/V rooms are coordinated locally at each Center. A/V rooms have the capability to connect to other video conferencing facilities either within or outside NASA's Network. As required, some external or off-network connections can be coordinated with the NTC.

The NTC provides the following services:

- Provides accurate support to schedules and forecasts.
- Provides conference monitoring as required.
- Performs certification testing and registration for new conference rooms.
- Maintains the A/V Conferencing Security Plan.
- Supports engineering with research, testing, and development for new capabilities and project implementations.

Maintenance of one Core Conference Rooms at each NASA Center is provided by CP. Labor for maintenance is CP provided, though customers will be asked to fund labor for major implementation projects, or justified Project expedites. Customers are responsible for funding travel for their designated projects. Conference rooms must be refreshed on schedule as provided by their initial installation package and have valid owner information in the correct Project Service Level Agreement (PSLA) to be supplied maintenance by CP. All estimates for new installations and refreshes will include the full vendor available equipment warranties. All incidents involving maintenance should be reported via the ESD. CP will respond to these incidents and determine the problem for resolution of equipment provided by CP.

- Full Service
 - Maintenance Policy of 5 year service
 - Support up to \$10K per Incident
 - Rooms transitioned into Full Service will be on a refresh schedule based on equipment installed dates
 - Contract SLA
 - CP system security plan (as applicable)
 - PSLA validation with Customer understanding of 5 year refresh rate and schedule
 - Once out of warranty, with no intent of refreshing, the room will be removed from the PSLA and Component replacement will be performed by NICS via funding from center work packages.
 - After transition, rooms not placed in Full Service will be considered Limited Service
- Limited Service

- Provide Center Customers time to acquire funding for refresh, or determine if decommissioning is a more suitable option.
- All rooms will be covered under a CP system security plan (as applicable)
- No SLA, and therefore will not follow Full-Service Incident workflow process
 - Repairs/replacements will be performed utilizing the Change Request (CRQ) process
 - If an equipment failure occurs, all costs, to include labor are charged to the Customer and funded by the Center. During any downtime, no spares will be utilized from the NICS pool
 - Customers have the option to obtain a quote for full support at any time
 - If equipment reaches end of life or fails to meet IT security requirements the rooms must be refreshed or be decommissioned and removed from the CP inventory and security plan
 - New options like wireless content sharing capabilities are not added to Limited Service rooms

CP 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 A/V systems reside are provided by the NASA Locations, and physical changes to the rooms are completed by the facilities organizations at the resident Center. A/V Conferencing Services coordinates with the appropriate service organizations to ensure the communications connectivity to the rooms are provided.

3.2.3 Voice Teleconferencing System (VoTS)

3.2.3.1 Service Description

CP 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, as well as non-reserved 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.



3.2.3.2 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.

3.2.3.3 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.

3.2.4 Audio Teleconferencing Systems

Audio 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 rooms have audio service, which can also be integrated.

3.2.4.1 Service Performance

Current performance parameters are in the following paragraph and in Appendix D, CP SLA Measures. 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.

- Audio Conference Incident Reporting

If a problem occurred that prevented the successful completion of the conference to your satisfaction, [please](#) contact the NASA Enterprise Service 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

For Service Maintenance, please see [Section 3.8 Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.2.5 Cable Plant Services

3.2.5.1 General Service Description

The CP, through the NICS contract, will provide Cable Plant services which include operation, maintenance, design & engineering, 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.

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.2.6 Emergency Warning System

3.2.6.1 General Service Description

The CP, through the NICS contract, 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.

3.2.6.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.2.7 Public Address System

3.2.7.1 General Service Description

CP through the NICS contract will operate and maintain the Public Address System. This includes the public address system service requests and trouble ticket resolution.

3.2.7.2 Service Performance

For Service Operations, please see [Section 3.7, Service Operations](#).

For Service Maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.3 Collaboration Services

3.3.1 DeskTop Mobile ViTS (DMV)

3.3.1.1 Service Description

The DMV service provides a desktop video service that allows Users to share voice, video and data between NASA standards-based 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 ESD.

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

DMV is available on Personal Computer (PC) or Macintosh (MAC) platforms and the desktop plugin is available via the Agency Consolidated End-User Services (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.

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

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

3.3.1.2 DMV Incident Reporting

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

3.3.1.3 Service Performance

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

For Service Operations, please see [Section 3.7, Service Operations](#).

For Service Maintenance, please see [Section 3.8, Service Maintenance](#).

3.3.2 Instant Meeting

This is CP'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 CP Service Owner.

Instant meeting accounts are requested via the NAMS system and are available in (3) different types;

- 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, and Puerto Rico).
- Global: allows standard in-country toll and toll free dialing from all international locations except China, Brazil, Malaysia, India, Philippines, and Taiwan.

- 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.
 - 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.

Instant meeting service information, including commonly asked questions can be found on the CP website at cso.nasa.gov

3.3.2.1 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

3.3.3 Internet Protocol TV (IPTV)

3.3.3.1 Service Description

The Internet Protocol Television (IPTV) project establishes a highly unified, secure, and cost effective enterprise solution that enables NASA users to consume video content in a standardized method, independent of location, and optimized to make use of NASA's networking infrastructure. The services meets current NASA requirements for existing IPTV-like systems.

3.3.3.2 IPTV Incident Reporting

TBD (CURRENTLY IN PROJECT MODE)

3.3.3.3 Service Performance

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

3.3.4 WebEx

3.3.4.1 Service Description

CP offers Cisco WebEx as a FedRAMP certified cloud-based platform that provides organizations with the ability to conduct more productive meetings. Participants can join meetings from most browsers, devices, and systems. The Service is integrated with the NASA LaunchPad for host authentication as well as meetings based on security type. WebEx provides audio, video and web conferencing and group messaging to Multipoint desktop sharing. The Service allows for recording, file download and closed captioning. CP's approach leverages existing processes and tools, providing efficiencies and continuity.

Service Security is met by three separate levels:

1. Unrestricted – Accessible by meeting password
2. NASA Attendee Validated – Authenticated via LaunchPad
3. NASA Invitation Only – Must be invited by host and be authenticated via LaunchPad

3.3.4.2 WebEx Incident Reporting

Tier I ESD

Tier II NTC

Tier III CP Engineering

3.3.4.3 Service Performance

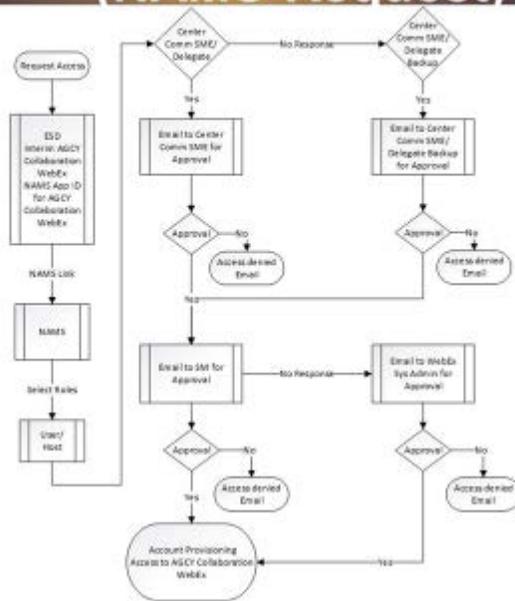
- The mean time to restore service for an in-progress conference shall be less than or equal to 4 hours.
- The mean time to restore service for non-conference impacting problems shall be less than 2 business days.
- Conference system availability shall be at least 99.5

3.3.4.4 Concept of Operations

1. After a NAMS request is generated, the Center WebEx Account Manager will validate and approve.
2. The request will then be assigned to the CP NICS WebEx Account Manager who will validate unassigned accounts to ensure a center does not over subscribe.
3. After validation is complete, the request is sent to be provisioned.
4. CP NICS WebEx Account Manager will generate reports and update Centers monthly.

NOTE: To cancel an account it is the reverse order.

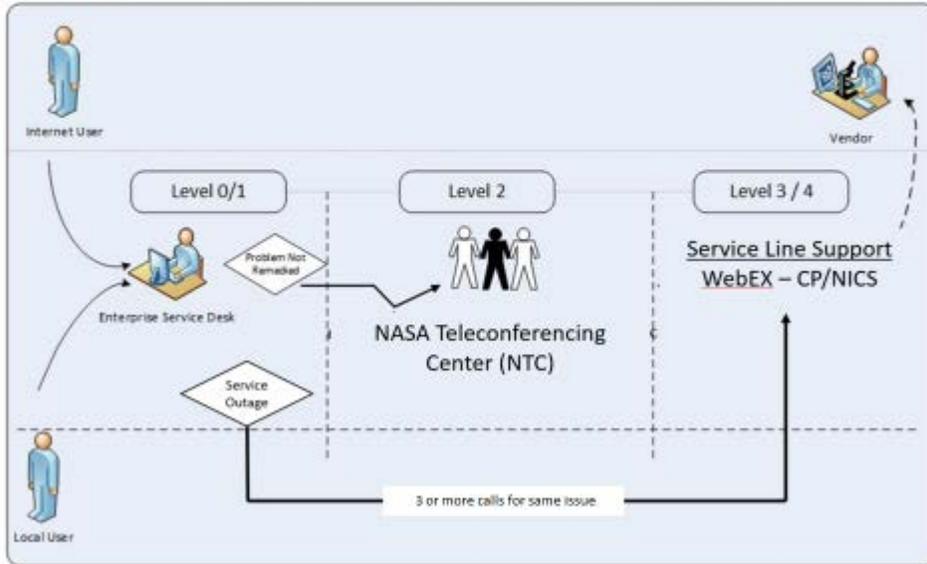
NASA CI Concept of Operations (NAMS Request)



DRR Template v0.1 20150520

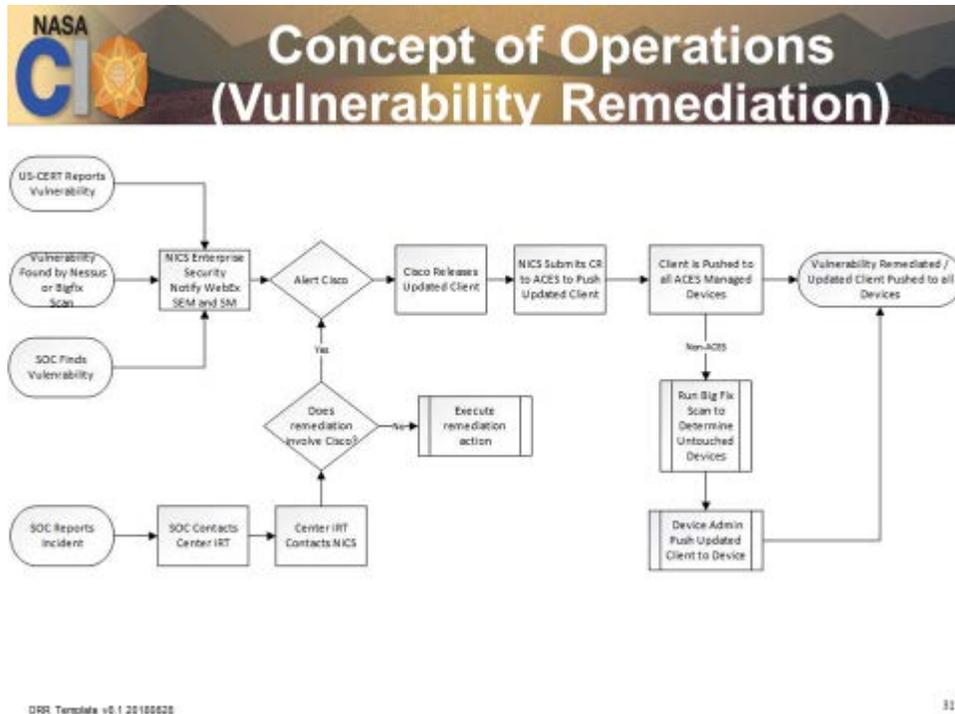
32

NASA CI Concept of Operations



DRR Template v0.1 20150520

33



3.3.5 Federal Relay Service

3.3.5.1 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 telecommunications conduits for the transmittal of information through Teletype (TTY), Videophone, Captioned Telephone (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 50 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.

3.3.5.1.1 Service Offerings

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

- Internet-Based Services:
 - Video Relay Service (VRS)
 - Internet Protocol (IP) Relay
 - Relay Conference Captioning (RCC)

3.3.5.2 Service Operations

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.*

3.3.5.2.1 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 as soon as possible prior to the scheduled event date and time.

3.4 Desk Telephone Services

3.4.1 Telephone Services

3.4.1.1 General Service Description

Communications Program (CP) provides the design, installation, operations, maintenance, and sustaining engineering for the voice systems at each NASA Center. This includes the implementation of voice service requests and incident resolution.

Voice services include Standard User and Admin type Desktop handsets with standard voicemail, Jabber Softphones with Visual Voicemail and telework capabilities, intelligent call routing supporting call center agents, local/long distance support, fax lines and analog service. Some Centers continue to support legacy TDM systems during migration to VoIP systems. Those Centers support basic TDM voice services to include desktop handsets, voice mail, local/long distance support, fax lines and analog service.

Service requests for voice service for each Center are requested by an ESD service request using the ESD Service Catalog. Incidents for any telephone services are opened by calling the ESD or using the online incident system. International dialing requires a separate service request.

3.4.1.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.4.2 Voice over Internet Protocol (VoIP) Service

3.4.2.1 General Service Description

CP, through the NICS contract, provides the design, installation, operations, maintenance, system engineering and sustaining engineering for the VoIP systems at all NASA Centers. This includes the implementation of telephone service requests and incident resolution.

VoIP telephone services include Standard User and Admin type Desktop handsets with standard voicemail, Jabber Softphones with Visual Voicemail and telework capabilities, intelligent call routing supporting call center agents, local/long distance support, fax lines and analog service. International dialing requires a separate service request. Service requests for VoIP telephone service at each Center are requested by an ESD service request using the ESD Service Catalog. Incidents for any telephone services are opened by calling the ESD or using their online incident system.

3.4.2.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

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

3.4.3.1 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.

3.4.3.2 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.

3.4.3.3 Calling Cards

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

3.4.3.4 Toll Free Services

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

3.4.3.5 Service Performance

The long distance (LD) service performance parameters will be consistent with the GSA Network contract terms.

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.5 Digital and Cable Services

3.5.1 DTV Support Services

3.5.1.1 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 CP PIP Routed data network.

3.5.1.1.1 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 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.

3.5.1.1.2 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

3.5.1.1.3 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

3.5.1.1.4 Human Exploration Operations Mission Directorate Channel (HEOMD)

- 7.25 Mbps via PIP network

- 24x7x365 availability
- MPEG-2 Compression

3.5.1.1.5 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 CP provides Six (6) video channels for use by NASA Centers/Projects and Remote Principal Investigator (RPI) locations via the Corporate Routed Data network. CP 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 PIP demarcation point. Service restoration for ISD resources is <8 hours on weekdays, and on-call on weekends. CP provides decoding equipment at the HOSC/MSFC Telescience Center (TSC), GRC TSC, CSA, GSFC Robotics Lab and the GSFC Space Servicing Center to deliver National Television Standards Committee (NTSC) video outputs. The RPI sites require the video to be delivered in IP format for viewing on a PC. Remote Principle Investigator (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.

3.5.1.2 Verizon AVOC Video Feeds

- 1.485 Gigabits per second (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 ISS Video Service transport in support of ISS Operations

3.5.2 Cable Television Services

3.5.2.1 General Service Description

CP, through the NICS contract, will operate, maintain, and perform sustaining engineering on the cable television distribution system. The contractor shall implement CATV service requests and perform trouble ticket resolution within the bands delineated below, and within the estimated/target cost of the contract.

3.5.2.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.6 Radio Communications Services

3.6.1 Radio Services

3.6.1.1 General Service Description

CP, through the NICS contract, 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.

3.6.1.2 Service Performance

For service operations, please see [Section 3.7, Service Operations](#).

For service maintenance, please see [Section 3.8, Service Maintenance](#).

For SLA information, please see [Appendix D, CP SLA Measures](#).

3.7 Service Operations

3.7.1 CP Services Management

CP services as designed and implemented typically include the capability to allow proactive monitoring, fault management, out-of-band access, metrics reporting, and configuration management. This provides the means to quickly identify and isolate problems that may include failures or degradation of service. Faults are reported to centralized management services and geographically diverse backup management services. Indication of faults including nature of alarm and severity are displayed on management systems monitored 24 x 7 by service management staff that review and respond appropriately to alarm conditions. Primary management of networked devices is performed through in-band secure communications sessions. Out-of-band access via diverse connectivity paths provides management access to core devices in the event a failure prevents in-band management access. Services are implemented to achieve service level targets and business continuity plans are maintained and exercised to help assure that service integrity is preserved during an event that renders primary physical, electrical or logical management infrastructure unusable.

3.7.2 MSFC Operations Center

The Operations Center at MSFC has primary responsibility for day-to-day Corporate-related systems/services. The MSFC Operation Center consists of the Corporate Network Operations Center (CNOC), NASA Teleconferencing Center (NTC), and Russia Services Group (RSVG). The Enterprise Service Desk (ESD) is responsible for first level Help Desk support and includes general

user interface and Incident administration. The CNOC is responsible for overall network management, including service implementation, sustaining operations, Incident and problem management, network maintenance activities, major outage notification, and network event alarm monitoring. The ESD can be reached by phone at 1-877-677-2123 or <https://esd.nasa.gov/esd/>.

The NASA NTC, located on-site at MSFC, provides video bridging support and acts as a back-up monitoring station for the vendor Video Bridging Service (VBS) during high visibility periods, such as select conferences related to ISS mission activities. The NTC hours of operation are Monday-Friday, 6am-5pm Central, and can be contacted at 256-961-9387 or 9388. The VBS can be contacted at 1-877-789-0670.

1. Onsite Operations support is provided by staff located at each NASA Center during normal business hours in most cases, but with on-call dispatch as needed.

3.7.3 GSFC Mission Services Operations

The Operation Center at GSFC, referred to as the NASA Communications (NASCOM) Operations Management Center (NOMC), has primary responsibility for day-to-day mission-related systems/services. The NOMC consists of the Communication Manager (COMMGR), and supports day-to-day network operation management; the Goddard Communications Control (GCC), responsible for router management, data circuit monitoring, carrier coordination and escalation, and Conversion Device (CD) operations; the Voice Technical Operations section, responsible for mission dedicated voice; and the NASCOM Network Scheduling Group (NNSG). The NOMC can be reached (301) 286-6141.

3.8 Service Maintenance

The Service Level Agreement supporting operations posture for a service is fortified, as appropriate, through vendor hardware maintenance, software licensing, and/or service agreements. Vendor maintenance agreements are reviewed regularly to ensure continued applicability to the reinforcement of a service posture and associated Service Level Agreement. Service Management monitors vendor performance to executed maintenance agreements and engages Supplier Management, as appropriate, to remediate vendor performance/delivery issues.

4. CP NASA Communications (NASCOM) Mission Network Services

4.1 Overview of the CP NASCOM Mission Network

The CP Mission Network is the Agency's ground communications infrastructure for spacecraft control and operations. It is comprised of a world-wide complex of systems and capabilities which have been designed to carry real-time mission data and voice services.

The Mission Network is comprised of NASA and commercial carrier managed services with equipment located at NASA, military, and contractor sites, as well as international sites that support human space flight (HSF) and other NASA Programs

The CP NASCOM Mission Network has been designed to provide these services on a 24x7x365 basis to HSF, ISS, Expendable Launch Vehicle (ELV), and Robotics (unmanned) missions between mission project control centers, launch complexes, international partners, and the ground stations of the Space Network (SN), Near Earth Network (NEN), and Deep Space Network (DSN).

Its critical services include transport of real-time telemetry and commands between ground stations and project control centers. The network also has an essential role in HSF, ISS visiting vehicle, and ELV launches. The Mission Network is managed primarily out of GSFC.

To fulfill its critical role in spacecraft operations, network availability and security are essential. The CP Mission Network has several characteristics that distinguish it from the CP Corporate Network, including:

- End-to-end redundancy with physical path diversity to support availability up to 99.98% with some services requiring as low as 1-minute service restoral.
- Security commensurate with conducting critical spacecraft operations and the need to prevent unauthorized access.
- Rigorous change control processes that support system freezes and formal freeze exemption process during critical support periods. The change control process actively coordinates with all NASCOM customers to minimize impact to spacecraft operations.
- On-console support during launches, landings, and critical coverage periods including spacewalks and planetary fly-bys.
- Administrative services including voice, video, data, and collaboration services.
- Operational support for:
 - Testing and simulation
 - Mission readiness
 - Pre-launch activities
 - Post-mission analysis and closeout

4.2 CP NASCOM Mission Network Service Management

The Mission Networks Division (MND), Code 770 at GSFC is responsible for provisioning and providing sustaining operations and maintenance support for the systems and services which comprise the CP NASCOM Mission Network operating environment.

4.3 Submitting Requirements for CP NASCOM Mission Network Services

The Mission Service Manager (MSM) group is the customer's primary point of contact when requesting CP NASCOM Mission Network-based services. In conjunction with a contractor Customer Services Representative (CSR)s, they serve as the focal point for gathering requirements, maintaining continual dialogue with customers and overseeing the service request process.

Customers requiring Mission Network services should contact the MSM group via email at GSFC-CSO-NASCOM-CIT@nasa.gov to discuss their requirements. MSMs and CSRs collaborate with NASCOM engineers and the customer to define solutions based on customer provided requirements.

4.4 CP NASCOM Mission Network Services

The CP Mission Network, NASCOM, is NASA's primary terrestrial ground network for supporting spacecraft operations. NASCOM is a world-wide complex of systems and capabilities used to provide data, voice, and video services between Mission project control centers, launch complexes, ground stations of the SN, NEN and DSN, and international partners.

NASCOM's role is to design, implement, and manage the Agency's Mission Network infrastructure to ensure the highest level of spacecraft ground communications operations and support.

The Mission Network is comprised of NASA and commercial carrier managed services with equipment located at NASA, military, and contractor sites, as well as international sites that support HSF and other NASA Programs. Its critical services include transport of real-time telemetry and commands between ground stations and project control centers. The network also has an essential role in HSF, ISS visiting vehicle, and ELV launches. The Mission Network is managed out of GSFC OCIO organization.

To fulfill its critical role in spacecraft operations, network availability and security are essential. The CP's Mission Network has several characteristics that distinguish it from the Corporate Network, including:

- End-to-end redundancy with physical path diversity to support availability up to 99.98% with some services requiring as low as 1 minute service restoration.
- Security commensurate with conducting critical spacecraft operations and the need to prevent unauthorized access.
- Rigorous change control processes that support system freezes and formal freeze exemption process during critical support periods. The change control process actively coordinates with all NASCOM customers to minimize impact to spacecraft operations.
- On-console support during launches, landings, and critical coverage periods including spacewalks and planetary fly-bys.
- Administrative services including voice, video, data, and collaboration services.
- Operational support on a 24x7x365 basis for:
 - Testing and simulation support
 - Mission readiness
 - Pre-launch support
 - Post-mission analysis and support

NASCOM can design, implement, and manage all, some, or none of the customer network infrastructure to assure the highest level of spacecraft operations support.

4.4.1 CP NASCOM Mission Network Layer-3 Transport

Layer-3 transport/Routed Data Service (previously referred to as Routed Data Service) is provided through a CP managed backbone infrastructure. Layer-3 provides switching and routing for transmitting data from node to node. Routing and forwarding are functions of layer-3 transport service, as well as addressing, internetworking, error handling, congestion control and sequencing.

4.4.2 Layer-3 Transport Embedded Components

The following components are part of the overall makeup of the CP NASCOM Mission Network. The following components are imbedded in the Layer-3 environment:

- CP NASCOM Mission NTP Management
- CP NASCOM Mission Network Secure Shell (SSH) Gateway
- CP NASCOM Mission Network Web Proxy
- CP NASCOM Mission Network Intrusion Detection System (IDS)
- CP NASCOM Mission Network Vulnerability Scanning
- CP NASCOM Mission Network Perimeter Firewall and Gateway Management

Other components available for use:

- CP NASCOM Mission Network Email
- CP NASCOM Mission Network Windows Server Update Service (WSUS) Management
- CP NASCOM Mission Network Anti-Virus Management
- DNS Management: DNS hostname and registration is provided by the Agency (NASA) through the CP under DDI (formerly IPAM)

4.4.3 CP NASCOM Mission Network Layer-2 Transport

Layer-2 transport/Dedicated Data Service is used to supplement Layer-3 transport/Routed Data Service. Layer-2 provides switching by creating logical paths, known as virtual circuits, for transmitting data from node to node. Layer-2 provides physical addressing, error correction, and preparing information for transport on the physical infrastructure. This is typically a point-to-point connection.

4.4.4 Mission Voice

The CP NASCOM Mission Voice Service supports voice conferencing between end-user devices and point-to-point connectivity between Agency mission voice switches based on customer defined requirements.

Voice conferencing provided by CP NASCOM is specific to connecting to the GSFC voice switch either by keysets or other Center voice systems (i.e., trunk interfaces).

4.5 CP NASCOM Mission Network Ancillary Services

4.5.1 Installation of Local, Customer Procured “Timing” Devices

Mission customers located at the Goddard Space Flight Center or the Wallops Flight Facility may request the installation of customer procured “timing” devices such as Greenwich Mean Time (GMT) clocks, Countdown Clocks, and Time Code Generators. Included in this Ancillary Service is engineering support, the installation of the “timing” device, cabling, and the configuration of the equipment needed to provide access to the required timing circuits. CP NASCOM Engineers provide a final timing device configuration solution based on customer specific requirements.

4.5.2 CP NASCOM Local, Mission Cabling Installation

NASCOM also offers local cabling support to its Goddard and Wallops customers. Local cabling may be provided for any segment between rooms, floors or buildings to connect customer(s) to existing infrastructure and/or equipment. Local cabling may also be ordered for the purpose of connecting customer provided equipment to the CP NASCOM Mission Network.

NASCOM can also provide user-only cabling upon request within customer enclaves. This cabling is not connected to the NASCOM Mission Network and is solely for the customers use.

4.5.3 CP NASCOM Mission Network Security Management

Security commensurate with conducting critical spacecraft control and the need to prevent unauthorized network access for the CP NASCOM Mission Network is provided by the Mission Operations Security Team (MOST). The MOST enforces a very constrained user behavior via monitoring and policing. Route and/or traffic filtering may be implemented to provide restricted access to certain sub-networks as indicated by mission ITS requirements.

Responsibility for maintaining the integrity of the network is shared with the customer. All systems, equipment and facilities which connect to CP NASCOM mission network and make use of its services are required to comply with the CP NASCOM Mission Network Security Policy, and all applicable NASA policies.

4.5.4 Operations and Maintenance Support

A standard feature of all NASCOM services is 24x7x365 operations and maintenance support. The CP NASCOM Mission Network Communications Manager (COMMGR) is the primary interface for incident reporting and coordination for operational activities. The direct line to the COMMGR is 301-286-6141.

Scheduled maintenance activities and configuration changes to the CP NASCOM Mission Network infrastructure are announced to the NASCOM user community in advance of the actual activity. In the event of a network outage or impairment of service, unscheduled “make operable” changes may be needed which require coordination with affected project(s). NASCOM utilizes rigorous change control processes which ensure that system freezes are enacted during critical coverage periods as mitigation to minimize risk to spacecraft operations.

4.6 Optional Support Provided by NASCOM

In addition to the standard services outlined above, NASCOM also provides support for Heightened Awareness”, which is Scientific Flyby’s, Orbit Adjustments, and Spacecraft Emergencies. NASCOM Support provided includes a Freeze of Network resources. No additional staffing support is provided.

Host Center Support

CP NASCOM Mission Network host Center support is an integral part of maintaining mission services which transverse through multiple geographically separated NASA telecommunications facilities. Host Center support is documented through agreements with the CP/MND that outline on-site support for troubleshooting, equipment resets, vendor escort, etc., that support CP NASCOM mission services which originate from GSFC. Host Center personnel subject matter experts possess vast experience necessary to effectively support troubleshooting and service restoration efforts.

Power and cabling are important factors in overall service availability for the CP NASCOM Mission Network. Critical network devices require redundant, diverse power sources, and where feasible, protection from the potential loss of commercial power. Customer facilities will be requested to provide redundant and diverse power service for the Mission Critical services terminating at those facilities. Consideration must also be given to communications cabling diversity to minimize potential single points of failure. Customer facilities will also be required to provide the proper environmental controls.

At GSFC, power, environmental and cable connectivity to the CP NASCOM Mission Network is controlled and installed by NASCOM to ensure that applicable security controls and configuration management are met.

At host Center sites other than GSFC where GSFC Communications Control (GCC)-managed equipment is to be installed, NASCOM works with site personnel to address power, environmental, provisioning and communications cabling diversity. Actual installation of cabling may be done by NASCOM or host site personnel, depending on customer and host site requirements.

4.7 Performance Standards for Layer-3 and Layer-2 Data Transport Service

Performance standards as stated are from CP NASCOM-managed Service Demarcation Points. Two performance categories for data transport services have been defined, Mission Real Time Critical and Mission Critical. Data Transport services are engineered to an Availability of no less than 99.95%.

- **Mission Real Time Critical**
 - A level of data networking connectivity with emphasis on meeting real time telemetry data transport. The Mission Real Time Critical performance category is engineered with a higher level of redundancy and diversity to support an availability measurement of 99.98% and higher priority for Restoration to Service (RTS) of less than 1 minute.

- **Mission Critical**
 - Mission Critical is differentiated from Mission Real Time Critical in that it is engineered with a lower level of redundancy and diversity resulting in a lower level of availability and lower priority for Return to Service (RTS). The Restore to Service time for Mission Critical services is 2 to 4 hours.

5. Russia Services

5.1 General Service Description

The Russia 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 Russian Federation, including the 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 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, and the 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.

5.2 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 NASA Information Support Center (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.

These services are maintained by CP and are provisioned as part of the service.

For SLA information, please see [Appendix D, CP SLA Measures](#).

6. How to Request CP Services (Corporate and Mission)

6.1 General

Customers can request CP services either by contacting the Center/Program representative, CSR or MSM. Additionally, a Customer can go directly to the ESD.

Requests for CP services shall be submitted to CP 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 PSLA used for Mission and Corporate Network requirements.

6.2 The Requirements Process

6.2.1 Customer Actions

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

- 1) Contact your CP SME, CSR or MSM (see Appendix F for a list of CP 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/CP/ CSR who shall be managing the processing and implementation of your requirement or (2) submit a SR form directly to the NICS/CP/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.
- 2) 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 ROM Costs and Detailed Cost Estimates are provided in Appendix F. The CSR will generate a SR for the requested ROM or Cost Estimate.
- 3) WAN service requests associated with Mission requirements shall be coordinated directly with the CP MSM group (SO) (see Appendix F for the name and phone number of the MSM that can assist you for your requirement). In conjunction with CSRs, they serve as the focal point for gathering mission requirements, maintaining continual dialogue with customers and overseeing the service request process. Customers requiring CP NASCOM Mission services should contact the MSM group via email at GSFC-CSO-NASCOM-CIT@nasa.gov to discuss their requirements. MSMs and CSRs collaborate with NASCOM engineers and the customer to define solutions based on customer provided requirements.
- 4) Designated personnel representing existing Data Center Network (DCN) customers may request adds, modifications, and changes to existing services via the DCN Service Request System (SRS). Services – other than routine requests supported by the ESD web site – must be submitted via the standard SR process.

- 5) As part of the NASA I3P Program, NASA established an ESD. The service Desk will process requests for all Corporate CP services. The ESD/ESRS provides Tier 0/1 Help Desk support services in response to reported incidents and problems and provides an integrated service ordering capability enterprise Service Request System (ESRS) for all CP Corporate and Center Communications services. The national number and Agency-wide contact information is as follows:
- a. By Phone: 1-877-677-2123
 - b. By e-mail: nasa-esd@mail.nasa.gov
 - c. On the Web: <https://esd.nasa.gov>

6.2.2 NASA CP 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. CP shall provide ROM costs and Detailed Cost Estimates upon request.

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

The distinctions between a ROM Cost and 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. Depending on the complexity of the request, 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, CP cannot set a general standard that would be applicable to all requests. Often, detailed information is required from sources outside CP and may only be gained by the issuance of a formal Request for Information (RFI) to industry. However, CP 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. CP Funding Methodology

7.1 *Customer Billing Guidelines for FY21 Bill and FY22-FY26 Projected Billing:*

- This methodology applies to all Communications Program (CP) services listed in the CP Services Document (CSD) located on our [website](#). Customers are defined as any Center, Mission Directorate, Mission Support Directorate, Staff Office, Program/Project and/or end user who requests CP services.
- The NICS contract that provides enterprise end-to-end communications and network infrastructure period-of-performance will end on May 31, 2021. In FY21, Centers will be required to provide resources to support Work Package (WP) development for the follow-on contract.
- Enterprise Infrastructure Solutions (EIS) – the Communications Program is migrating General Service Administration (GSA) Networx services to the new federally mandated GSA EIS contract. **This contract change will affect billing, funding, service levels, vendors, service pricing and/or credits. Customers should closely review their bills for changes.** CP does not anticipate any disruption in service and we will provide ongoing communications to ensure a smooth transition.
 - Due to this transition, customer funding for impacted Program Service Level Agreements (PSLAs) should be provided in monthly/quarterly increments.
 - Customers **may also be responsible for dual operations costs** during the period of transition. This overlap should be for no more than 60 – 90 days while the circuits move from the existing contract to the new contract.
- CP termination liability policy states that the customer is responsible for payment during the 60-day period after notification is received by CP. For other periods or delayed disconnect requests, CP will negotiate a reasonable time to assure customer expectations can be met.
- Mission Operations Voice Enhancement (MOVE) Maintenance: Beginning FY21, some customers may need to fund MOVE Maintenance, as communicated in the PPBE22 Strategic

Program Guidance (SPG). CP will communicate funding requirements directly to customers and via the FY21 IT Resource Analyst (RA) Summary.

-
- Additionally, if maintenance is continued under NICS, the Local Site Administrator (LSA) upgrade will be required.
- Mission Next Generation Voice (MNGV) Systems: The Communications Program (CP) has established an Agency contract vehicle to allow the purchase of Mission Next Generation Voice (MNGV) systems and capability to replace existing Agency mission voice systems. Centers and Mission Operations should coordinate with CP to work through anticipated budget requirements for this replacement at their sites. Center MOVE maintenance costs are independent of MNGV implementations.
- The CP Enterprise License Agreement (ELA) which covers licensing for VoIP end devices, SIP licensing for center to center calling, ISE licensing for NASA end devices, intrusion protection (IPS) licensing, and VPN Anyconnect licensing for the agency is currently being renegotiated. The vendor has changed their pricing model which will require full funding to be provided at the beginning of the POP.
- CP will incorporate the existing billing totals for Mission Infrastructure Services for the utilization, operations and maintenance of the NASCOM Network located at GSFC (formerly known as Local Mission Comm) into the PSLA. This will provide a single combined bill for those GSFC CP customers. More information provided in the “What you pay for” section below.
- Virtual Private Network Services (VPNS) – CP anticipates an increase in VPNS usage as NASA transitions to EIS. Requirements added onto an existing shared service, i.e. VPNS or E-Line that require an incremental upgrade of the existing service, will be funded by the requesting customer. The Project will fund the full incremental increase for the base period. Recurring funding distribution for shared services will be prorated for each FY according to the bandwidth required.
 - A requested service may include shared access on one or both ends.
 - Disconnect of a shared service may result in continued cost until the end of the FY.
 - If a portion of the service is unique to the requesting Project, this cost will follow the CP termination liability policy.
 - Shared VPNS costs may vary (higher or lower) from PSLA cycle to PSLA cycle depending on the number of users requiring the connection and the capacity increments available from the vendor.
- Local voice services currently not on the NICS contract are being moved under CP prior to the Session Initiation Protocol (SIP) transition which falls under EIS. Centers will be responsible for the continued funding of their local voice services once the transition to SIP

is complete. Details are still being finalized for the post-SIP transition cost breakout to the Centers.

- WebEx service pricing for the Centers will be based on a snapshot of the current Host accounts along with growth estimates provided by the Center Comm SME at the time of the data call.
- Center-funded services transitioning into an Enterprise Service Line under the NICS contract will continue to be funded by the Center until funds are realigned to CP.
- 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. NICS 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 users of the contract 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.
- For **FY21-FY26** WPs, CP will apply escalation factors outlined in the NICS contract.
- For **FY21-FY26**, CP 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 PSLAs. Cost estimates for new room installations are available upon request.
- CP 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 and schedule the room for decommission.
- The initial installation of a SR/CRQ-driven, CP Collaboration Facility includes maintenance for all systems in the room up to \$10K per incident for five years. Any incident 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, unless on the schedule for refresh; it will be removed from PSLA and be supported on a limited service basis with no service level guarantees.

- Rooms across the Agency that are absorbed from other contracts or local providers will be considered as limited service support with all repair costs funded by the customer unless refreshed by CP via the SR/CRQ process and become a CP Collaboration room under PSLA.
- A “Video Conferencing Usage” charge for the ViTS bridging/ops service will be charged to JPL and NSSC based on the prior year video conferencing usage. If applicable, any monthly/usage charges for Integrated Services Digital Network (ISDN) services that support these Center-funded ViTS will also be charged to JPL and NSSC.
- CP will no longer be providing Desktop Mobile ViTS (DMV) as a service effective 9/30/2020.
- Each Center is responsible for ordering and funding NEST services consistent with the job requirements for the NICS employees located at the Center.

CP FY21 Funding Strategy:

What you pay for:

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

- All OCONUS except SN, DSN, and NEN
- Tail Circuits
- MOVE Maintenance for Center switches and keysets (see above)
 - At GSFC, Mission Projects requiring MOVE keysets will fund the purchase and associated maintenance for the keysets
- LSA upgrades for Center MOVE equipment (see above)
- MNGV Switches and keysets (with associated maintenance) for Center mission voice systems (see above)
 - At GSFC, Mission Projects requiring MNGV keysets will fund the purchase and associated maintenance of the keysets
- Virtual Private Network Service (VPNS)
- Custom Services
- Customized Data Center Network (DCN)
- Replacement equipment for both Video and Voice Conferencing rooms
- Center services supported by CP NICS (e.g. Radio, Limited Service Collaboration Rooms)

- NEST services for NICS employees resident at the Center are considered Center-funded Funding for these services was not realigned to CP
- ELA maintenance costs
- WebEx Host accounts allocated to your Center
- Local voice services currently being transitioned to CP in support of conversion to SIP
- Closed Captioning costs in excess of defined Center allocations.
- Any new/missed requirements which fall under the Service Lines not included in the PPBE17 funds realignment
- All Center Infrastructure Development, Modernization and Enhancement (DME)
- JPL and NSSC only:
 - Current and Future ViTS over ISDN monthly cost and usage
 - Video Conferencing usage
- JPL, SSC and VAFB only:
 - Switched Voice
- NSSC only:
 - Shared Corporate Enterprise Work Packages (Center allocation)
 - Service Line Work Packages (Center allocation)
- SSC only:
 - VoIP operations and support
- GSFC only:
 - Mission Projects will fund Mission Infrastructure Services for the utilization, operations and maintenance of the NASCOM Network located at GSFC.
 - GSFC Mission Infrastructure Services Fee for use of dedicated and shared small conversion devices
 - GSFC Mission Infrastructure Services Fee for use of mission voice infrastructure
 - Unique Statements of Work (SOW)

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
- For Mission Services:
 - Unforecasted requirements for Simplified configurations and routing changes

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 IT Business Services (ITBS) 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 ITBS Contracting Officer.
 - This method will be used for all CP services
 - See attached listing of Center IT RAs.
- The ITBS 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 ITBS PPBE21 data call. Updates to this schedule will be provided by the ITBS as needed for new requirements not included in the original projections.

What CP funds:

CP will be responsible for funding the following services (except for named exceptions listed in the “What you pay for” section above):

- Requirements that are in the CP Operating Plan
- WAN Mission Services for the SCaN Network:
 - Space Network (SN)
 - Deep Space Network (DSN)
 - Near Earth Network (NEN)
- Collaboration Services:
 - Voice Teleconferencing Service (VoTS) Usage (Instant Meeting Service and reserved service)
 - Video Conferencing usage
 - Sustaining engineering and labor for all CP 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 Element Manager and the Center Comm SME. Centers are responsible for providing suitable room upkeep in regards to HVAC, power, and furniture.
 - Refresh and maintenance support for one ViTS Gateway test bed per Center.
- Shared Corporate Enterprise Work Packages
- Service Line Work Packages (WPs):
 - Operations and Maintenance (but not DME) for local Communications Services (i.e. LAN, Telephone and Cable Plant)
- NEST seats for NICS contractor employees (excluding seats funded by Centers for NICS staff resident at the Centers as funds were not realigned to the Program).
- ELA maintenance for CP Projects’ support
- Closed Captioning (defined, limited allotment per Center)
- Web Content Filter and VPN
- Data Center Network (DCN) for designated Agency Enterprise Data Centers
- MOVE Maintenance for NASCOM infrastructure switches and keysets
- Continuation of maintenance agreement under Frequentis USA MOVE contract until each switch expires
- Development cost for LSA upgrade for the MOVE environment
- LSA upgrades for NASCOM MOVE infrastructure
- MNGV Switches and keysets (with associated maintenance) for NASCOM infrastructure
- VPNS for existing CP funded services
- WebEx Host accounts for CP and NICS contractor employees funded within the CP internal budgets

Appendix A. Acronyms

Acronym	Description
AAO	Agency Applications Office
ADP	Automatic Data Processing
ACES	Agency Consolidated End-User Services
AES	Advanced Encryption Standard
AFRC	Armstrong Flight Research Center
ALS	Agency Logging Solution
AOPNS	Activity, Outage Plan Notification System (retired system)
APL	Approved Product List
ARC	Ames Research Center
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASI	Asynchronous Serial Interface
ASN	Autonomous System Number
AVOC	Audio/Video Operations Center
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CAPTEL	Captioned Telephone
CATV	Cable Television
CAWG	Communication Architecture Working Group
CENMS	Corporate Enterprise Network Management System
CFO	Chief Financial Officer
CIEF	Carrier Independent Exchange Facility
CIO	Chief Information Officer
CMDB	Configuration Management Database
CNOC	Corporate Network Operations Center
COMMGR	(CP NASCOM Mission Network) Communications Manager
CONUS	Continental United States
COTS	Commercial-off-the-shelf
CP	Communications Program

Acronym	Description
CRQ	Change Request
CSONS	Communications Service Office Notification System
CSDM	Customer Service Delivery Manager
CSR	Customer Service Representative
CTA	Communications Target Architecture
DCN	Document Change Notice
DCN	Data Center Network
DDI	DNS, DHCP, and IP address management
DHCP	Dynamic Host Configuration Protocol
DL	Distribution List
DMR	Detailed Mission Requirements
DNS	Domain Name System
DME	Development, Modernization, and Enhancement
DMZ	Demilitarized Zone
DSN	Deep Space Network
DVA	Desktop ViTS Appliance
DVB-S	Digital Video Broadcasting - Satellite
EIGRP	Enhanced Interior Gateway Routing Protocol
EIS	Enterprise Infrastructure Solutions
E-mail	Electronic mail
ELA	Enterprise License Agreement
ELV	Expendable Launch Vehicle
ESD	Enterprise Service Desk
ESRS	Enterprise Service Request System
EWS	Emergency Warning System
FCD	Funds Commitment Document
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
Gbps	Gigabits per second
GCC	GSFC Communications Control
GISS	Goddard Institute for Space Studies

Acronym	Description
GMT	Greenwich Mean Time
GN	Ground Network
GPS	Global Positioning Satellite
GSA	General Service Administration
GSFC	Goddard Space Flight Center
HQ	Headquarters
HSF	Human Space Flight
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IONet	Internet Protocol Operational Network
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISD	Information Systems Directorate
ISP	Internet Service Provider
ISS	International Space Station
IT	Information Technology
ITBS	IT Business Services
iTMS	Integrated Telecommunications Management System
IT RA	IT Resource Analysis
ITU	International Teleconferencing Union
JSC	Johnson Space Center
Kbps	Kilobits per second
KSC	Kennedy Space Center
LAN	Local Area Network
LD	Long Distance
LIMS	Live Interactive Media Service
LMR	Land Mobile Radio

Acronym	Description
Mac	Macintosh
MAC	Media Access Control
Mbps	Megabits per second
MCDTV	Multi-Channel Digital Television
MCU	Multipoint Control Unit
MCM	Mission Communications Manager
MND	Mission Network Division
MOA	Memorandum of Agreement
MONS	Mission Outage Notification System (retired 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
NAC	Network Access Control
NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NASCOM	NASA Communications (CP Mission Network)
NDC	NASA Data Center
NEN	Near Earth Network
NGFW	Next Generation Firewall
NICS	NASA Integrated Communications Services
NID	NASA Interim Directive
NISC	NASA Information Support Center
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPD	NASA Policy Directive
NPR	NASA Procedure Requirements
NSSC	NASA Shared Services Center
NTC	NASA Teleconferencing Center
NTSC	National Television Standards Committee
NTP	Network Timing Protocol

Acronym	Description
OCIO	Office of the Chief Information Officer
OCONUS	Outside Continental United States
OCSS	Office of Cyber Security Services
OMB	Office of Management and Budget
OSPF	Open Shortest Path First
PBX	Private Branch Exchange
PC	Personal Computer
PIN	Personal Identification Number
PING	Packet Inter-Network Groper
PIP	Premium IP
POC	Point of Contact
PPBE	Planning, Programming, Budget, and Execution
PRD	Program Requirements Document
PRI	Primary Rate Interface
PSLA	Project Service Level Agreement
RAS	Remote Access Service
RCC	Relay Conference Captioning
RFI	Request For Information
RIP	Routing Information Protocol
RPI	Remote Principle Investigator
ROM	Rough Order of Magnitude
RR	Resource Record
RTS	Return To Service
SAP	Systems Applications Products
SCaN	Space Communication and Navigation
SEM	Service Element Manager
SIEM	Security Information and Event Management
SIP	Standard IP
SLA	Service Level Agreement
SME	Subject Matter Expert
SN	Space Network
SOC	Security Operations Center

Acronym	Description
SONET	Synchronous Optical Networking
SOP	Standard Operating Procedures
SR	Service Request
SRS	Service Request System (for DCN)
SSH	Secure Shell
STS	Speech-to-Speech
SVS	Switched Voice Service(s)
TLS	Transport Layer Security
TSC	Telescience Center
TTY	Teletype
UDP	User Datagram Protocol
UTC	Universal Time
VAFB	Vandenberg Air Force Base
VI	Video Interpreters
ViTS	Video Teleconferencing Service
VoIP	Voice over Internet Protocol
VoTS	Voice Teleconferencing Service
VPN	Virtual Private Network
VRA	ViTS Roll-About
VRS	Video Relay Service
WAF	Web Application firewall
WAN	Wide Area Network
WCF	Web Content Filter
WFF	Wallops Flight Facility
WP	Work Package
WSC	White Sands Complex
WSTF	White Sands Test Facility
WSUS	Windows Server Update Service

Appendix B. Definitions

Term	Definition
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.
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.
Demarc	Demarcation point for CP services, where customer equipment meets CP equipment
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).
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

Term	Definition
	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.
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.
Maximum Transmission Unit	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 data network and are not the CP default at the CP Customer facing interface. Increases to the CP routed data network default MTU sizing at the Customer demarcation point and the Customer CP facing interface is increased on a case by case basis.
Packet Loss	Packets transmitted from the source CP/Customer interface, i.e., the connection between the CP router and the Customer router, but not received at the destination CP/Customer interface. Acceptable loss is measured over any 24-hour interval.
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, CP uses an average of 100 packets each sent with a 36 byte payload.

Term	Definition
Switched	services in which communications resources are shared among many users using a switching device.
Tail Circuit	The circuit extension between the CP Backbone and the CP service demarcation at the Customer location. A tail circuit is typically Customer funded.
Time to restore	<p>CP shall make every effort through its contractors and carriers to restore interrupted service in a timely manner. A requirement has been levied by CP on itself, its contractors and its carriers to return CP services to an operational state as indicated in Appendix D.</p> <p>PIP and SIP time to restore is based on a calculated mean. MTTR for PIP and SIP services is calculated on outage data gathered in the proceeding 90 days and is based on the time CP 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.</p> <p>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.</p>
Validation	The authentication and confirmation by CP 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.

Appendix C. Supported Interfaces and Protocols

C.1 General

CP supports the interfaces and protocols listed below. If your particular requirement does not appear on this list, please contact 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).

C.2 Interfaces

Table 5: Supported 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			

C.3 Protocols

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

Table 6: Supported Protocols

User Data Protocol/Internet Protocol (UDP/IP)	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)	VOIP

Appendix D. CP Services Service Level Agreement (SLA) Measures

Service	Availability % ₁	Rtn to Svc (MAC) ₃	Coverage Period	Round Trip Time ₂	Acceptable packet Loss	(MTU) Bytes ₅	Standard Changes	Notes
Cable TV	99.7	8 business hours	M-F 6am-6pm					
Cable TV Display		8 business hours	M-F 6am-6pm					
Cable TV Display MAC		3 business days	M-F 6am-6pm					
Center Cable Plant-Inside		1 business day						
Center Cable Plant-MAC		3 business days	M-F 6am-6pm					
Center Cable Plant - Outside		3 business days						
Corporate Data Premium and Standard	99.99	4hr MTTR	24x7	<100ms	<0.001	1500		
Corporate LAN	99.90	TBD	24x7	<10ms				Jitter:≤ 5ms
DCN Premium	99.99	4hr MTTR	24x7		<0.001		<24hrs	All DCN standard changes <24hrs
DDI Services	99.99		24x7	Intra <50ms Extra <500ms				1 business day for DNS record changes
Emergency Warning System	99.7		24x7					
Guest Network Services	99.9		24x7					

CP-001 CSD v5

Service	Availability % ₁	Rtn to Svc (MAC) ₃	Coverage Period	Round Trip Time ₂	Acceptable packet Loss	(MTU) Bytes ₅	Standard Changes	Notes
Radio Services		2 business days	M-F 6am-6pm					
Remote Access Services	99.9		24x7					
Switched Voice	99.5	<4hrs MTTR	24x7					Probability of call block <1% or better
Telephone Service	99.9	4hrs	24x7					
Telephone Service Handset		8 business hours	M-F 6am-6pm					
Telephone – Handset MAC		3 business days	M-F 6am-6pm					
VITS- Custom, VRA, DVA	99.5	<4 hrs in progress <2 business days non-impacting						Supports up to 20 NASA locations in 1-10 simultaneous
VOIP	99.9	4hrs	24x7					
VOIP Handset		8 business hours	M-F 6am-6pm					
VOIP Handset MAC		3 business days	M-F 6am-6pm					
VoTS in progress conference	99.95	4hr	M-F 6am-6pm					Impacted conferences; <9 month Non-Conference
Russia Svcs Admin Data	99.95	<4hrs		<300ms				<1 percent packet loss
Russia Svcs Admin Video	99.95	<4hrs		<300ms				
Russia Svcs Admin Voice Fax	99.5	<4hrs		<300ms				P3 grade of service

CP-001 CSD v5

Service	Availability % ₁	Rtn to Svc (MAC) ₃	Coverage Period	Round Trip Time ₂	Acceptable packet Loss	(MTU) Bytes ₅	Standard Changes	Notes
Russia Svcs Msn Critical Data	99.98	<1min ₄		<300ms	<.001% loss			Capability to immediately switch to
Russia Svcs Msn Critical Voice	99.98	<5min ₄		<700ms				<1% Harmonic distortion <-40dbm0 noise level
Russia Svcs Msn Non-Critical Voice	99.95	<2hrs ₄		<700ms				<-40dbm0 noise level
Russia Service Msn/Admin Video	99.95	<4hrs		<300ms				
Russia Svcs Non-Critical Data	99.95	<2hrs		<300ms				<.001 percent packet loss
CP NASCOM MSN NW Layer-2 Transport MSN Critical	99.95	,2hrs	24x7					
CP NASCOM MSN NW Layer-2 Transport Real time MSN Critical	99.98	<1 min ₄	24x7					
Msn Routed Data Custom	Project Specified	Project Specified	24x7	<120ms CONUS	0.001	1500		
CP NASCOM Mission Network Layer-3 Transport MSN Critical	99.95	2hr-4hr	24x7					
CP NASCOM Mission Network Layer-3 Transport Real time MSN Critical	99.98	<1min ₄	24x7					
LabNet On-Premises	99.5	4hr MTTR	24x7	<120ms	<0.001	1500		
LabNet Off-Premises	99.0	24hr MTTR	24x7	<180ms	<0.005	1500		

Footnotes – CP Services Service Level Agreement (SLA) Measures

¹These values apply only for those parts of the WAN service supported by the CP 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.

²Round Trip Time (latency) is specified for data flow between domestic WAN nodes controlled and operated by CP. 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.

³These 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.

⁴ A capability for immediately switching to an alternate data path shall exist.

⁵ Mission data services jumbo frames of up to 9,000 bytes can be supported at some locations.

E.2 Standard Interval Factors

The CP 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 CP service Standard Intervals.

Many CP 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. CP 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 CP service implementation may impact completion dates.

CP 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 7: CP Service Planning Timeframes

Service	Design Phase	Implementation Phase	Total
VIDEO			
Custom ViTS	25	80	105
VRA/DVA	25	70	95
VOICE			
Custom VoTS	25	67	92
Switched Voice Service (ISDN BRI,PRI)	11	42	53
Toll Free Numbers	0	20	20
Mission Dedicated Voice	32	64	96
Dedicated Data			
Mission Dedicated Data	34	81	115

Service	Design Phase	Implementation Phase	Total
Dedicated Data	20	77	97
Routed Data			
Mission Routed Data	34	81	115
Corporate Routed Data	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 F. NASA CP Points of Contact (POC)

F.1 NASA Mission Directorate and Mission Support Offices

CP 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 bases. MSM/CSR assignments, for Corporate or Mission services, are found at; <https://cso.nasa.gov/under-contacts>. Where resources permit, the CP assigns both a primary and alternate person to be the cognizant MSM and CSR for each NASA Program, Center or Facility.

F.2 CP On-site Customer Support

CP provides CSR personnel who are co-located with the Customer and provide on-site support for CP services. A listing may be found on the CP website at:

<https://cso.nasa.gov/content/how-contact-us>

F.3 About this Document

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

Appendix G. Key Personnel

G.1 CP Center/Program Representatives

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

G.2 CP Service Element Managers (SEM)

The CP service owners can be found at the following website: <https://CSO.nasa.gov> under contacts.

Appendix H. NAMS Instructions for Access to CP/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://idmax.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 Q Type All Center All

Request Sponsor: Collins, Gregory A 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 CSO NICS SharePoint Q Type All Center All

Title	ID	Description	Type	Center
AGCY CSO-NICS SharePoint	233642	CSO/NICS collaboration environment.	IT Asset	MSFC

4. Via the "AGCY CSO-NICS Sharepoint" page, scroll down to the **Create Request** section and
 - a. Select "Urgency" level
 - b. Provide ***Business Justification** details
 - c. Please select the SharePoint Site(s) and Permissions (Read Only or Contributor) required

CAWG
CAWG - Contributor

Collaboration Services Engineering
None

Comm SME
Comm SME - Read Only

Configuration Mgmt Office Internal (for CMO employees only)
None

Contract Integration - Telecom Svcs
Contract Integration - Telecom Svcs - Re

5. Click **Submit Request** button.

Once access has been approved and provisioned, you will receive a completion notification from NAMS

Appendix I. NASA CP IT Security Check lists

I1. Security Check Lists Overview

New users of services must complete a NASA IT security checklist to connect to CP networks. The specific checklists are tailored to reflect the risks but as a general rule, the following areas must be addressed:

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

I2. The End User Security Assessment Form

The End User Security Assessment Form checklist is utilized for Corporate network connections (tail site) 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.

I3. The Mission Network Internet Protocol Operational Network (IONet) security checklist forms

The Mission Network IONet Security forms are utilized for access to the CP NASCOM Mission Network and can be found at.

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