Request for Proposal
for
Selection of Agency for Upgradation and Operations & Maintenance of Gujarat State Wide Area Network (GSWAN) and Gujarat State Data Centre (GSDC)

Department of Science & Technology (DST)

Government of Gujarat

Volume-II

(Scope of Work and SLAs)

(RFP No. GIL/H&N/DST/GSWAN_GSDC O&M/2015)

Bid Processing fees: Rs. 25,000/-

Pre Bid Meeting: 19/09/2015
Last Date for Bid Submission: 12/10/2015
Bid Opening: 13/10/2015

Gujarat Informatics Ltd
Block no. 1, 8th floor, Udyog Bhavan,
Sector-11, Gandhinagar-382017, Gujarat
Ph No. 23259237, 23259240
Fax: 23238925. Email: info@gujaratinformatics.com
www.gujaratinformatics.com

Section I: Introduction

1. Gujarat State Wide Area Network (GSWAN)

Government of Gujarat implemented the Gujarat State Wide Area Network (GSWAN) in the year 2001-02. The end-to-end IP based network was designed for the service convergence (Voice, video and Data) on the same backbone. The key objectives were:

- To modernize the intra-governmental communication setup
- To improve administrative effectiveness and efficiency
- To facilitate improvements in the Quality of Public services

1.1 GSWAN Overview

- Government of Gujarat implemented the Gujarat State Wide Area Network (GSWAN) in the year 2001-02. The end-to-end IP based network was designed for catering G2G Data and Video services on the same backbone.
- GSWAN is one of the largest IP based Multi Service IT infrastructure connecting all Districts and Talukas to State capital Gandhinagar.
- More than 5,000 Horizontal Office locations of Government and semi-government offices are connected with GSWAN.
- All District Centers (DC) are connected to State Capital (SC) through 34 Mbps Leased Circuits aggregating at the State Data Centre (SDC).
- All Taluka Centers (TC) are connected to respective DC through 10 Mbps Leased Circuits.
- All DCs are interconnected through 34 Mbps Leased Circuits for redundancy.
- GSWAN at present has a user base of over 50,000.
- Core Internet Bandwidth of 1 Gbps through National Knowledge Network (NKN), 90 + 26 Mbps through two redundant Internet Service Providers.
- More than 200 Websites and Applications accessible to users hosted at State Data Center through GSWAN.
- More than 250 Video Conferencing End Points and 8 Multi Conferencing Units (MCU's) are operational on GSWAN.

1.2 Existing Network Architecture

- The network topology as conceived and designed for GSWAN was based on a hub-and-spoke design topology, with three tiers in to it. Essentially, the network was designed primarily for G2G services and linear hierarchical approach had been followed for application/resource access :

First tier	Secretariat Center (SC)	• Secretariat Center (SC) at state capital, Gandhinagar, where from the highest office of Government functions in the state. • Various departments and hundreds of subordinate offices located at the state capital are connected to SC horizontally through SCAN (Secretariat Campus Area Network). • SCAN has about 8000 Ethernet extensions at Gandhinagar and all these are interconnected with GSWAN at SDC level for information exchange. • 300 GSWAN Hotline phone connections have been provided to various offices at Secretariat for direct voice communication to

		any GSWAN node in the state (at District or Taluka level).
Second Tier	**District Centers (DC)**	• Second Tier constitutes District Centers (DCs) located at district collector's office and multiple district level other offices connected with DC horizontally. • All 33 DC's are connected on 34 Mbps leased lines with SC. • Gandhinagar DC is a part of SCAN infrastructure. • GoG evaluated several options to achieve cost effective, flexible and scalable connectivity for all horizontal offices and used Cat-5, OFC, JFC, wireless VSAT on case to case basis.
Third Tier	**Taluka Centers (TC)**	• Third Tier constitutes Taluka Centers (TCs), located at Taluka Mamlatdar office and Taluka Development Office. • At TCs provision are kept for connecting Taluka level other offices horizontally. • All Talukas are connected to DC with 10 MB Leased Lines from BSNL. • In each of the stations, there is a state-of-the-art Router, which terminates the Leased Line. These routers route IP packets intelligently throughout the network, and provide the Quality of Service (or QoS) features to enable convergence of voice, video and data on to a single network infrastructure.

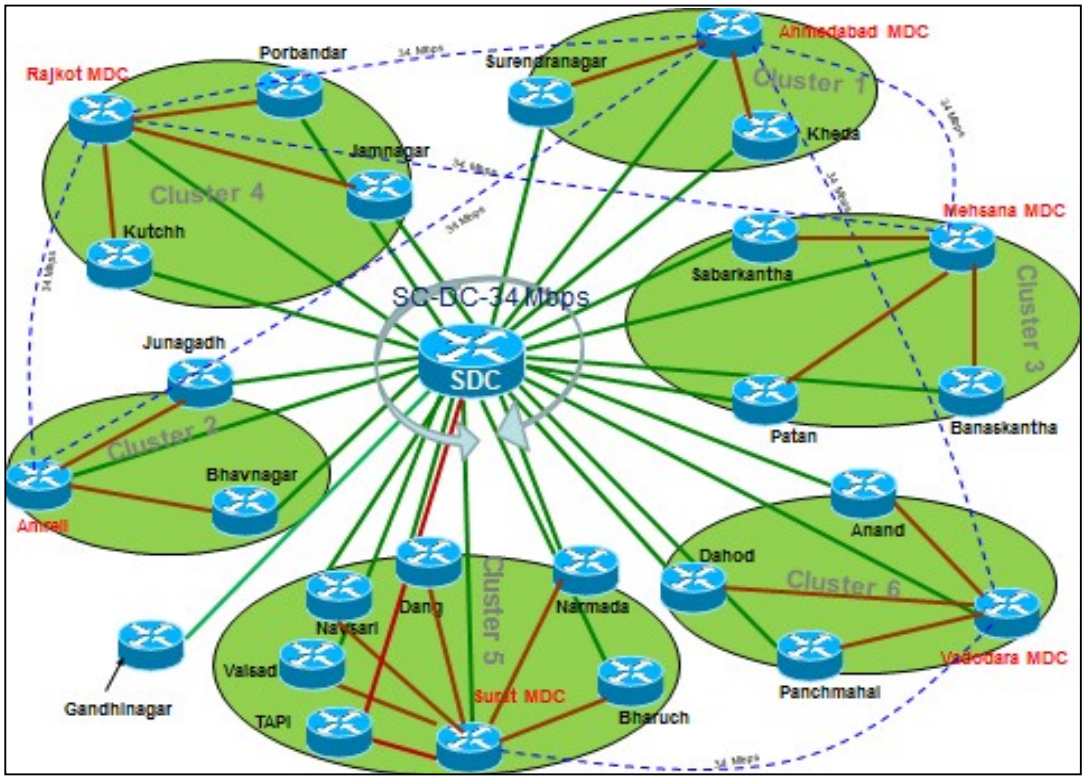

Fig 1.1 Existing Network Overview

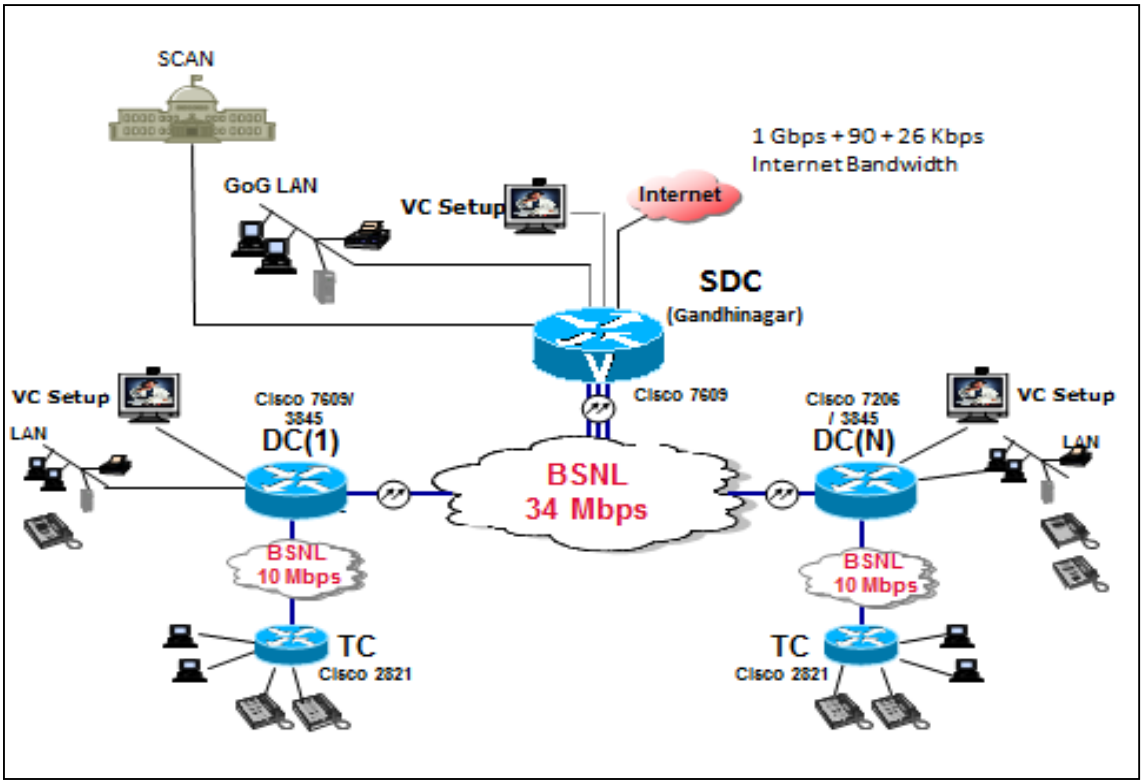

Fig 1.2 Existing Network – Tier I & II

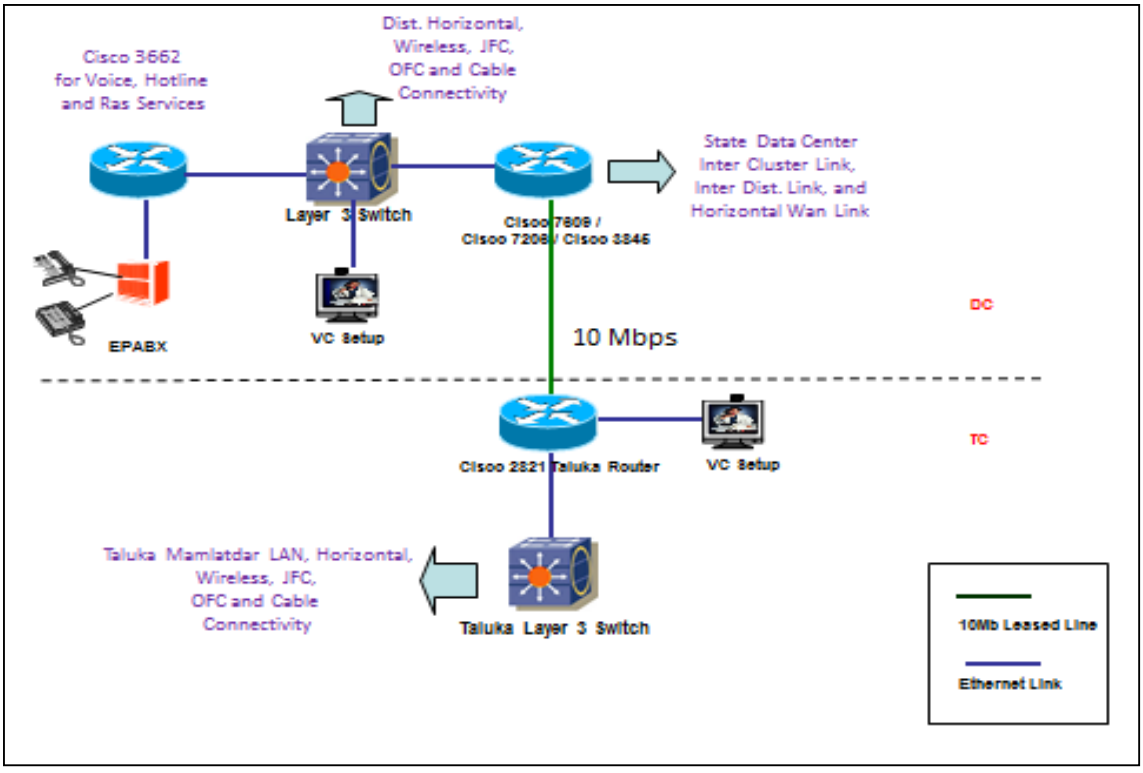

Fig 1.3 Existing Network – Tier II & IIII

1.3 Proposed Network Architecture

Upgraded GSWAN is envisaged to be a MPLS (Multi-Protocol Label Switching) based network architecture.

Multiprotocol Label Switching (MPLS) will enable GSWAN to be upgraded as next-generation intelligent network that can deliver a wide variety of advanced, value-added services. User departments with differing access links can be aggregated on an MPLS edge without changing their current environments, as MPLS is independent of access technologies.

- Integration of MPLS application components, including Layer 3 Network, Layer 2 Network, Traffic Engineering, Quality of Service (QoS) and IPv6 will enable creation of a highly efficient, scalable, and secure GSWAN that will guarantee Service Level Uptime and Availability.

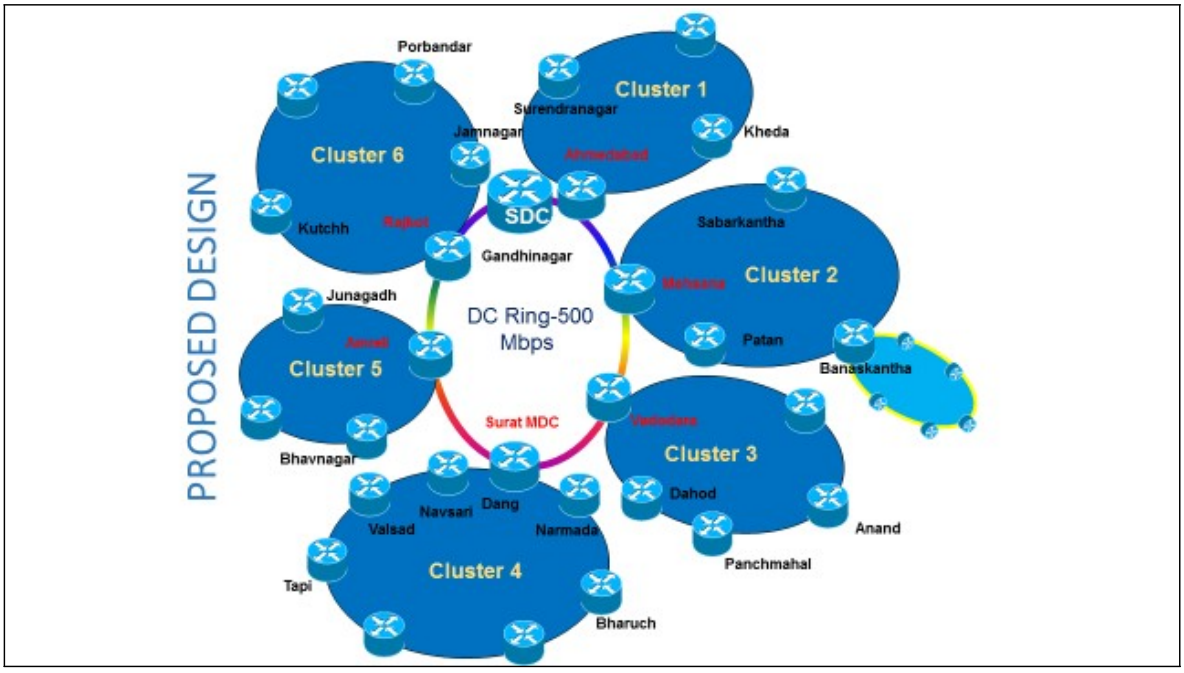

Fig 1.4 Proposed Core Network on MPLS

2 Gujarat State Data Centre (GSDC)

Government of Gujarat has set up Gujarat State Data Center (GSDC) in Gandhinagar, the State capital. GSDC includes 2600 sq.ft of server & storage area, 600 sq.ft of connectivity zone and 1300 sq.ft of control room & utility area. GSDC has been connected to all the Government offices through GSWAN infrastructure and is operationalized since 2008.

2.1 GSDC Overview:

Server and Storage Area:	• Capacity to put 82 full height (42U) Racks

2600 Sq. ft	• Co-location/hosting of approx. 300+ Servers from various State Government Departments • Hosting of approx. 300+ Government websites and Applications • Storage capacity of approx. 900+ TB to store State Government and Citizen's critical information/data • Two sets of UPSs of 240 KVA capacity each to provide battery backup
Connectivity Zone (Network Room): **600 Sq. ft**	• Firewall • Intrusion Prevention System • DMZ (Demilitarized zone) • Load Balancer for multiple ISP's link • Routers and Layer 2/3 switches for network
Control Room and Utility Area: **1300 Sq. ft**	• UPSs and Battery banks • Panel Switches • Precision Air conditioners (PAC) • FM 200 Gas cylinders to protect against fire situation • Building Management System • 24 x 7 x 365 CCTV/Surveillance monitoring system • Water Leakage Detection System • Rodent repellent system • Access Control System • Fire Alarm System/Smoke Detection System
Network Operation Center (NOC) Area: 2500 Sq. ft	• 24x7 Monitoring and Management facility for GSDC and GSWAN • Operations and Management Team Seating arrangement for approx. 50+ personnel

Section II: Scope of Work

The scope of work under this RFP is broadly divided into two components:

- System Integration Component: Upgradation of IT and Non-IT Infrastructure under GSWAN and GSDC.
- Operations & Maintenance Component: O&M of IT and Non-IT Infrastructure under GSWAN and GSDC.

2.1 Upgradation of IT & Non-IT Infrastructure in GSWAN & GSDC

The bidder is required to Supply, Install, Commission, integrate and upgrade network devices in GSWAN and GSDC as per the specifications mentioned in the Bid document and buy-back the old items that are replaced. The bidder shall ensure the seamless integration and interoperability with existing installed GSWAN and GSDC infrastructure and shall provide declaration on seamless integration.

2.1.1 The bidder shall design the upgraded network on ring architecture with three rings connecting Secretariat Centre (SC) to 6 Clusters (Ahmedabad, Vadodara, Surat, Rajkot, Mahesana and Amreli) with 250+250 Mbps bandwidth, District Centre (DC) to District Centre (DC) ring (33 Districts) with 250+250 Mbps bandwidth and Taluka Centre (TC) to Taluka Centre (TC) ring with 100/200 Mbps bandwidth and three hundreds PoPs on 50/100 Mbps bandwidth.

2.1.2 The bidder shall install, configure, integrate and commission all the systems as per the technical specifications mentioned in Section VI of Vol-I of the RFP.

2.1.3 The bidder shall depute adequate skilled resources to ensure that the implementation and commissioning activities are carried out on schedule.

2.1.4 The bidder shall submit a detailed test plan and test cases for each solution, that will be used to carry out the UAT (user acceptance test) and FAT (final acceptance test)

2.1.5 As part of the project completion documentation, the bidder shall submit the documentation, which should at least contain

(a) As-implemented configurations

(b) As-implemented architecture and topology diagrams

(c) Standard operating procedures for administration of the installed devices.

2.1.6 The bidder is required to carry out following tasks**:**

(a) Currently there are about 60,000 users on GSWAN. This number is expected to increase to 1.5 L in future course as GSWAN is being expanded rapidly, The Bidder must size and configure the Network devices being supplied in this bid accordingly. The specifications mentioned in the bid are to ensure functional performance of the network components.

(b) It is envisaged that all Routers connected on Ring architecture till TC level will run MPLS. The bidder needs to design the network architecture accordingly using best industry practices.

(c) GoG has implemented a centralized WLAN Controller (CISCO 8500 Series) at SDC, Wi-Fi will be provided to selected offices and key users on GSWAN under this project. The Successful bidder will Supply and Install the access points. GoG will decide locations for installation of Access Points. The Bidder will be responsible for Installation, configuration and complete O&M of the same. GSWAN user ID and Password will be used to provide authentication to users over Wi-Fi.

(d) Currently the GSWAN works on Static IP schema. The successful Bidder will implement DHCP IP plan at all offices of GSWAN. MAC ID of every machine (Desktop/Laptop) will have to be automatically detected and bound with IP address to enable plug and play access for users. For Mobile/Tablet users, GSWAN services would be available through pre-defined authentication. The gateway Router of the District should learn the MAC and store in its table.

(e) **Site Preparation: -** The Successful bidder is solely responsible for Site preparation as per the local requirements. The bidder is expected to carry out necessary civil works to ensure standardization of sites in terms of layout and facilities and will have to provide all civil, electrical, passive infrastructures.

(f) **Migration Plan: -** The bidder will have to ensure successful migration without disturbing the existing services running on GSWAN and GSDC. The bidder will have to suggest the migration plan for the same and will have to obtain an approval from GoG, before implementation.

2.2 Operations and Maintenance (O&M) of GSWAN

2.2.1 The Successful bidder shall be responsible for the overall management of the IT and

Non-IT Infrastructure and enabling infrastructure maintenance services / facility management services at all GSWAN locations for ensuring adherence of SLAs. Bidder shall integrate with the existing EMS tool at the State Data Centre that monitors / manages the entire enterprise wide application, infrastructure and network related components. Bidder shall provide the Operations and Maintenance Services for a period of 5 years following the award of the contract. The bidder shall be responsible for following:

(a) The Successful bidder shall be responsible for operating and maintaining the network for connectivity between Secretariat Centre (SC), District Centre (DC) and offices connected with DC horizontally (approx. 70 to 80 offices per DC) and Taluka Centre (TC) and office connected with TC horizontally (approx 20 offices per TC). The successful bidder is responsible for operating and maintaining network of SC, all 33 DCs and 248 TCs, all MS Buildings and PoPs (list enclosed) and future horizontal connectivity provided/to be provided by DST.

(b) For better Network availability, preventive maintenance activity is required to be carried out at least once in a quarter which includes configuration backup and software up gradation/updation.

(c) Successful Bidder is required to submit preventive maintenance schedule of all equipments to DST. After performing preventive maintenance activities, bidder is required to submit the report of the same. All such activities should be done preferably in non-working hours.

(d) As part of the Operations and Maintenance services, the bidder shall provide support for the software, hardware, and other infrastructure provided as part of this RFP. Bidder shall also provide 5 years comprehensive AMC. The bidder shall also provide services comprising of but not limiting to the following:

    (i) Operations and maintenance services for existing and new IT and Non-IT Infrastructure supplied or commissioned by the bidder at the GSDC and SC, DC, TC and other PoP locations in GSWAN for five years during the contract period.

    (ii) Support for the end users at each of the DC and TC locations including

deployment of one competent person per location for the entire period of the contract.

(iii) Other IT infrastructure related support services for five years from signing of the contract.

(iv) The services shall be rendered onsite from the designated premises. To provide the support at the locations where the infrastructure will be rolled out, bidder is expected to provide experienced and skilled personnel at each location.

(d) Warranty Support

As part of the warranty services bidder shall provide:

(i) Bidder shall provide a comprehensive warranty and on-site free service warranty for 5 years from the date of FAT for all equipments.

(ii) Bidder shall obtain the 5 year product warranty and 5 year onsite free service warranty from OEM on all licensed software, computer hardware, peripherals, networking equipment and other equipment for providing warranty support.

(iii) Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.

(iv) Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

(v) Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period bidder shall replace or augment or procure higher-level new equipment or additional licenses at no

additional cost in case the procured hardware or software is not adequate to meet the service levels.

(vi) Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipments for inspection, delivery of equipments or for commissioning of the systems or for acceptance tests / checks on per site basis, DST/GIL reserves the right to charge a penalty.

(vii) During the warranty period bidder shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidders notice.

(viii) The bidder shall as far as possible repair/ replace the equipment at site.

(ix) In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC the unserviceable HDD will be property of DST/GIL and will not be returned to bidder.

(x) Warranty should not become void, if DST/GIL buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.

(xi) The bidder shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.

(xii) Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

(xiii) Bidder shall ensure that the warranty complies with the agreed

Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

(xiv) Bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

(xv) Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

(xvi) Bidder shall develop and maintain an inventory database to include the registered hardware warranties.

(xvii) Bidder shall also be responsible for the comprehensive AMC of existing IT Infrastructure. Details of the existing hardware which may be required to be covered under AMC by the selected bidder through this RFP are attached as Annexure "A", Annexure "D" and Annexure "E". Currently some of the hardware is under AMC cover, however bidder will be required to provide AMC post expiry of existing AMC cover.

2.3 Network operations, Services and maintenance

2.3.1 The services as per the scope of the contract shall include maintaining the network equipment; ensuring running of the services (Data, Voice, and Video) with availability in line with the SLA and Round-the-clock Network monitoring. This shall include:

(a) Equipment Configuration Management
(b) Upgrading IOS
(c) Maintaining access control list
(d) Regular review of Network
(e) Regular reports as required by DST and authorized agency from SC, DC & TC
(f) Regular backup of NMS server
(g) Monitor GSWAN Network at SC, DC, TC & Cluster Level

(h) Regular reports as required by DST & authorized agency from SC, DC, TC & Cluster Level

(i) Auto backup configuration of Router and Switches for SC, DC, & TC

(j) Regular SLA Violation reports for Network vendors

(k) Upgrading Patches on all equipment's including NMS-Servers, network & Security Devices and hardening of network & security devices.

(l) The Successful bidder is required to maintain uptime of the network between SC, DC, TC and other PoPs to meet the SLA .In case the network uptime is not maintained due to non-availability of link/Bandwidth by Service provider, bidder is required to produce documentary proof (Service Desk Complaints/Incidents or Vendor assigned Tickets) in terms of certificate of downtime of network link/b/w from the service providers. In case bidder fails to provide such documentary proof the same shall be treated as non- performance of SLA and would be liable for penalty.

(m) The Successful bidder shall keep the details of all the Assets and document any changes in the assets including up-gradation and/or replacement of assets. The asset inventory for the entire network architecture shall always be up to date and shall be submitted to DST on quarterly basis.

(n) Bidder is required to keep requisite spares to ensure adherence of SLAs and continuity of O&M operations

(o) Successful bidder will have to do operational liasoning with stake holders (link providers, state government, local bodies, third party agencies / consultants appointed/identified by GoG) to keep the link up & running.

(p) Successful bidder should deploy adequate resources at DC & TC to provide operation, maintenance and support services. Scope of services at DC & TC would include following:

(i) Fault detection in equipment's at DC, TC, other PoPs, Horizontal Offices

(ii) Analysis and follow-up in case of network connectivity issues and vendor managed services (Leased lines, RF and LAN) till the level of field offices

(iii) Coordinating with LAN cabling vendor for repairs in the LAN network

(iv) Carry out feasibility survey for new connectivity

(v) Network Configuration of user device and connecting it GSWAN network

(vi) Coordinating with Central Help Desk to resolve the trouble tickets to meet the SLAs

(vii) Carrying out the FAT and certifying the work completion carried out by sub-vendors

(viii) Bidder would be responsible for providing network connectivity at every computer as SLA, bidder will not be responsible for providing application/ Desktop support.

(q) **Comprehensive Annual Maintenance Contract of out of warranty network equipment at SC, DC, TC and other PoPs:** Successful bidder shall enter into comprehensive AMC contract for out of warranty equipment/ hardware at SC, DC, TC & other PoPs. List of existing devices, which are not being changed/replaced, and for which currently AMC is either not available or will expire during the Contract period of this bid, is placed at Annexure "A" and Annexure "D", bidder will have to provide AMC for these items till the end of this contract.

(r) In case DST/GIL decides to migrate the network to IPv6, the successful bidder shall prepare the migration plan and execute the same within 21 working days.

(s) Successful bidder is responsible to facilitate services for video conferencing to end-user offices located at SC, DC or TC or any other office across the State. Presently VC equipments are installed at all District Collectors Offices, all Taluka Mamlatdar offices and at Sachivalaya Campus. For such events, O&M team shall test the setup and report after the completion of events. Nonperformance under this clause will result into penalty.

(t) DST/GIL is providing GSWAN Connectivity for web casting services to various remote places across the State for events of Dignitaries through last mile connectivity provided by ISP/Wireless Vendor. Successful bidder is responsible for managing and coordinating these events. Successful bidder is required to keep requisite skilled resources having background of Web Casting and Video Conferencing. Non-performance under this clause will result into penalty.

(u) Successful bidder will help and co-ordinate with DST/GIL for paying electricity bills of SC, DC, TC and other PoPs on behalf of DST/GIL and actual amount of electricity bills will be reimbursed by DST/GIL along with the Quarterly O&M Payment.

(v) Bidder has to provide UPS & Battery Health Reports in every quarter after completing proactive maintenance every quarter. Bidder will have to replace batteries at the end of 2nd and 4th year of the contract period during 9th and 17th quarter.

(w) DST/GIL has set-up control room at State Centre at Gandhinagar and District Centers at District Collector offices across the State. Successful bidder has to ensure the following for smooth running and operation of the systems at SC, DC, TC & other PoPs, as prescribed.

(i) Cooling requirement of the operational equipment at DC control room need to be maintained. For this purpose Bidder shall deploy Automatic cut-off device to switch between the Two ACs installed. Bidder shall monitor the environment variables of the control room through the Infrastructure Management System (IMS) supplied in this bid to ensure uninterrupted operations at all DCs.

(ii) Proper electrification along with proper earthing and anti-static flooring, structured cabling for proper management of cables need to be maintained at SC, DC, TC & other PoPs. Bidder has to ensure proper earthing at any point of time during O&M Operations. Proper earthing of Neutral to Earth Voltage less than 1.5 Volts has to be maintained and tested on monthly basis.

(iii) Cabling with proper tagging as per cabling standards with network diagrams need to be maintained at SC, DC, TC & other PoPs.

(iv) Bidder shall deploy Building Management System (BMS) with features of rodent repellent, fire detection and extinguisher and water leakage detection and prevention and ensure Cleanliness, hygiene and safety at DC, TC & other PoPs.

(v) Bidder shall deploy Access Control System and maintain record of access, man and material movement for the DC control room.

(x) Successful bidder shall be responsible for providing technical feasibility report along with Cable route diagram, LAN sitting arrangement and diagram, digging permission status in case of JFC/OFC connectivity and permission status for mast installation in case of wireless connectivity for expansion and laying of new horizontal link/PoPs and effort estimation and cost-estimation for the same to the DST/GIL. This work has to be performed within the prescribed time-limit of 7 working days. Bidder has to follow Change Management documentation, while submitting new location report, along with capacity Report for new location. Non adherence to time-limit will result into penalty.

(y) Successful bidder shall be responsible for carrying out FAT of the work carried out for expansion and laying of new horizontal link/PoPs by all sub-vendors and will provide recommendation for payment for the said work.

2.4 Network Planning, Optimization and Expansion Services

2.4.1 Core Network

(a) The network should have the capability and facility for Seamless integration with GoI initiatives like NII 2.0, NOFN.

(b) Network must support next generation architecture to support future application like IP based Surveillance, Voice, Video, Wi-Fi etc.

(c) All the proposed routing devices should support key IP MPLS feature and protocol for enablement of same as and when required.

(d) Network will be connected in Ring architecture and devices must support the redundancy protocol for better convergence.

(e) The Ring Based architecture must be deployed to meet the following:
   (i) Redundancy of nodes and Links
   (ii) Less prone to failures
   (iii) Better Link utilization
   (iv) Traffic should not Hog core bandwidth for any to any communication
   (v) Easy Insertion of new Node. No configuration change at Core

(f) Core network must support Node and Link protection feature for faster and reliable network convergence.

(g) MPLS Traffic Engineering feature must be deployed at TC and DC Routers.

(h) MPLS Traffic Engineering should be used to Provide the following:

(i) Bandwidth guarantee for critical real-time applications in the control plane.
(ii) Optimized utilization of redundant links between DC and the core.
(iii) Handling of unanticipated load in the network.
(iv) Uneven utilization of links.

(i) TC and DC Network must support resource reservation protocol (RSVP) based dedicated path For Critical Application.

(j) Network Convergence methods like MPLS Fast Reroute (FRR-Link and Node) and Bidirectional failure detection needs to be deployed to achieve faster convergence.

(k) TC and DC Routers should support IPv4 Fast Reroute to reduce the routing transition time to less than 50 milliseconds during a link failure.

(l) SC and DC Routers should support BGP fast convergence feature for IP and MPLS-VPN to improve BGP convergence after network failure. This convergence should be applicable to both core and edge failures and can be used in both IP and MPLS networks. The BGP fast convergence feature for IP and MPLS-VPN feature must create and store a backup/alternate path in the routing information base (RIB), and forwarding information base (FIB) so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover.

(m) The network will be running OSPF as an IGP protocol and features like Route Summarization should be supported to reduce the number of routes in neighboring routers.

(n) Router must be configured for Multi Area IGP topology as per network requirement.

(o) IGP should be only used for carrying management routes and user routes should be shared using Broader gateway protocol (BGP)

(p) Routers must support segregation of departmental traffic using Virtual Routing and Forwarding (VRF).

(q) Routers must support Hub and Spoke, MESH and Extranet VPN as per requirement of network.

(r) Network must support BGP for IPv4, IPv6 and VPNv4.

(s) All Internet exit will be from SDC.

(t) Proposed solution must consider NAT to facilitate IPv4 NAT, IPv6 to IPv4NAT VRF Aware NAT to meet end user requirement.

(u) Route Reflector based BGP Solution should be designed keeping scalability in consideration.

(v) Route Reflector must be scalable and devices proposed as Route Reflector must support high routing scale in a small form factor.

(w) Network must have two Route Reflectors for redundancy however bidders are free to quote more.

(x) QoS enables a network to provide improved service to selected network traffic. The Network must support the following MPLS QoS features:

(i) MPLS Experimental Field
(ii) Classification
(iii) Policing and Marking
(iv) Preserving IP ToS

(y) At least 4 Class of diff-serve based Service Model should be deployed.

(z) Standard methods such as ACL, IPP, DSCP & MPLS EXP should be used for classifying the traffic.

(aa) Congestion avoidance methodology such as WRED should be deployed in conjunction with QOS to meet optimal performance in network.

(bb) All devices in network should support Hierarchical Quality of Service for Ingress and Egress.

(cc) All devices should support priority queuing for assigning more priority to Voice and Video traffic over non critical data traffic.

(dd) The network should support Multiprotocol BGP based methodology to carry IPv6 with in a MPLS VPN over an IPv4 MPLS network to ensure no additional overhead is put on Routers.

(ee) The proposed design should not require any change in SC and DC Router configuration for IPV6 transport and should run only IPv4 protocols.

(ff) The Taluka and POP Router shall support adaptive routing for path selection using link performance criteria like Response time, packet loss, delay, jitter and traffic load of Wan links for intelligently controlling the traffic and to maximize the quality of the user experience

(gg) The Taluka and Pop router should also facilitate application based performance monitoring and automated routing control of traffic in case SLA is breached.

(hh) All the devices in network must support DHCP relay functionalities.

(ii) Switching devices must provide security for ipv6 network/links similar way that of ipv4 network.

2.4.2 The successful bidder will provide on-going support to GSWAN for specific network planning and optimization services such as configuration support required for addition of new sites and locations to the network, VLAN creations, and voice/data/video / services, upgrading to IPv6 from existing IPv4, improving network availability and performance and capacity planning services. This may include following specific activities:

(a) Provide inputs for network expansion including effort estimation and cost – estimation.

(b) Up gradation of SC, DC, TC & PoP network from IPv4 to IPV6 using latest technology (Dual Stacking, Bridging, Encrypted Tunnel preparation etc.)

(c) Update technical design documents on quarterly basis.

(d) Configuration of network hardware and software and planning for implementation.

(e) Create a checklist of activities to be performed for technical network operations

(f) Successful bidder will ensure IP network is monitored for performance and utilization of the network resources, including monitoring of the IP network and equipment for it's over or under utilization, and provides capacity reports to optimize and commission the B/W or equipment accordingly.

(g) Evaluate the utilization of all the IP network and check for the adequate bandwidth provisioning.

2.5 Network Management Processes

2.5.1 The Gujarat State Wide Area Network (GSWAN), should be managed in accordance with various standards e.g. ISO Network Management Model (ISO20000: latest version), ITIL, Disaster Recovery Model, OEM Certifications for AMC & Services for GSWAN etc. For this purpose, processes may be defined under following functional areas that would govern the GSWAN Network Management:

(a) Configuration management
(b) Performance management
(c) Fault management
(d) Backup management
(e) Network Security Management
(f) Network Redundancy Management
(g) Change Management

2.6 EMS/NMS for SLA and Performance Reporting

2.6.1 The Successful bidder shall operate and maintain an Enterprise Management Suite (EMS)/Network Management System (NMS) and SLA and Performance Monitoring System for GSWAN backbone at Network Operation Centre (NOC) and GSDC components centrally at SC. Currently GSWAN is monitored through CA-NMS tool version 6.3 and GSDC is monitored through CA-NMS (as per Annexure"F"). The successful bidder will have to replace this tool with appropriate equivalent NMS tool with equal or better capabilities on taking over the O&M Operations. The EMS/NMS tool should provide Supervision and Call Centre support for GSWAN and GSDC. The new tool should be managed by the Successful Bidder for the complete contract period and shall be used for regular monitoring of the network. Successful bidder shall configure/ provision the systems to be used by GoG for audits and also help in monitoring the service level parameters on an ongoing basis as defined in Service level agreements. The DST/GIL or its designated agency shall have access to all generated

reports for service levels audits and monitoring. Successful bidder shall deploy adequate access policy and security policy on the systems in consultation with DST/GIL for ensuring authenticity and integrity of the reports. The system shall essentially have 3 components, Network and Data Centre Management component, Helpdesk & SLA Management component. The DST/GIL or its designated agency should be able to view the SLA Management component. The Successful bidder shall be responsible for creating network monitoring environment through the following:

(a) The EMS/NMS system shall be configured to automatically discover all manageable elements of the GSWAN and GSDC.

(b) All network components shall be configured to alert the centralized EMS/NMS server in case of any events, so as to reflect real status of all network components and links across GSWAN and GSDC.

(c) The NMS should also poll all network devices and other IT and Non-IT components in GSWAN & GSDC at regular intervals in order to determine their status and working.

2.6.2 The functional requirements of the EMS/NMS system are as follows:

(a) **Alarm Correlation & Root Cause Analysis Capabilities**

(i) Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed by means of intelligent alarm correlation, suppression and root cause analysis techniques built in to the system. The system must ensure reduction in MTTR by means of advanced event correlation, filtering and root cause analysis.

(ii) It should have capability to perform cross domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool and other domain monitoring tools.

(iii) Alarm Filtering should allow flexible filtering rules for NOC staff to filter the alarms by category, severity, elements, duration, by user, by views, by geography or by department.

(iv) Ability to apply severity to alarms according to predefined rules.

(v) It should be possible to add description to the alarms.

(vi) The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause

analysis.

(vii) The system should be able to clearly identify configuration changes as root cause of network problems

(viii) Alarms should be mapped to the live topology views and real time updates to topology based on alarm occurrences.

(ix) Historical Reporting of alarms must be possible and system should be able to store large volumes of alarm data for historical reporting purpose

(x) It should be possible to convert Critical Alarms into Incidents for auto ticket generation into proposed Helpdesk tool.

(xi) Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.

(xii) Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.

(xiii) Consolidated network view embedded with digital maps

(b) **Network Fault and Performance Management**

(i) The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.

(ii) The Network Management function should have a graphical topological display of all discovered network devices in real time.

(iii) The proposed Network Fault Management solution must also provide network asset inventory reports

(iv) It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across GSDC/GSWAN and any further Network connectivity's planned in future by simple addition of required licenses without any change in topology.

(v) The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms

(vi) The discovery must also support device redundancy discovery in case of virtual IP addresses using vendor specific protocols such as VRRP and HSRP.

(vii) The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices. When a report is run the administrator must have an option of specifying the number of consecutive days the port must be "unused" in order for it to be considered "available".

(viii) The proposed solution must provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed management system must also intelligently determine which ports are operationally dormant. This will help in analyzing capacity needs of the Network ports and better network capacity planning across the GSWAN network.

(ix) It should support integrated Fault, Performance, and Configuration Management features from a single solution.

(x) It should show live interface connections between discovered network devices and must be able to do mapping of LAN and WAN connectivity with granular visibility up to individual port levels

(xi) It should proactively analyze problems to improve network performance.

(xii) The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display.

(xiii) The Network Management function should poll or collect and analyze the large volumes of fault and performance data. Once collected, it should automatically store data gathered in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and performance analysis.

(xiv) The Network Management function should have a feature of discriminated polling of devices.

(xv) The Network Management function should be able to monitor device performance in near real time

(xvi) It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.

(xvii) Solution should have a provision for suppression of maintenance alarms during the maintenance period.

(xviii) The proposed performance management system shall integrate

network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.

(xix) The proposed solution must scale to large networks while supporting a single web interface for access to reports. The system must support multiple locations and a distributed deployment for collection and monitoring. Primary instrumentation should exist at the Central Site.

(xx) The Proposed solution must support out of the box trend reports on group of metrics or group of devices in a single report. This will help understand the performance of multiple devices against a KPI (Key Performance Indicator)

(xxi) The proposed solution must support out of the box capacity planning reports that assist in the analysis of capacity needs based on projected load.

(c) **Network Performance Reporting**

(i) Solution should be able to collect Key performance measurements and statistics from all network domains and store it. This data is to be used for evaluation of performance of the end to end network infrastructure/services.

(ii) Solution should have functionality for KPI calculation on the raw metrics collected.

(iii) Solution should be able to do Trend analysis from the performance data.

(iv) Should be able to generate web-based reports both near real time and historical data for the network.

(v) It should be possible to view live report.

(vi) Solution should support historical storage of aggregated data for one year and data backup.

(vii) Proposed solution should be able to also provide a threshold and profile capability on the KPIs monitored on the network in order to understand the impact of failures and degradations which eventually results in downtime/network unavailability.

(viii) The system shall be able to support separate warning and violation threshold levels, so that in the event of gradual service quality

deterioration, warnings shall be generated before critical level thresholds are breached.

(ix) Out of the box fault and performance reports

(x) Customizable Reporting should be possible without the need for additional reporting engine.

(xi) It should support automatic base lining on historical data, and thresholds that can be adjusted as required, based on data collected.

(xii) It should have a secured interface with role based access and privileges.

(xiii) Availability of drill-down reports.

(xiv) Solution should offer off-the-shelf Reports for KPIs such as Availability, Uptime, and Resource Utilization.

(xv) Solution should have the capability to export the reports results in standard file formats like CSV, pdf etc.

(xvi) Should be able to present the reports through web and also generate "pdf" / CSV / reports of the same.

(xvii) Solution should have capability of exporting report in open interface formats for business intelligence tools, excel, etc.

(xviii) Solution should support capability to periodically generate (scheduled reports) and distribute statistics reports to the designated team members at customer side.

(xix) Solution should provide options to perform progressive trend analysis with multiple fixed time windows like 1 day, 1 week, 2 weeks, 1 month, 6 months etc.

(xx) Solution should allow configuring threshold crossing alerts on KPIs. It shall be possible to define threshold profile i.e. +/- variations around a given baseline for raw counters or KPIs/KQIs and generate alarms or threshold crossing alerts which would be forwarded to the Fault Management system or Event Correlation Engine.

(xxi) Solution should support retrieval of historical performance data collected at any monitored point and archived on the server. The solution should allow aggregation of historical data.

(xxii) Solution should facilitate reports summarized by time – Hour, Day, Week, Month, Quarter, Year and by Property- service, location, department etc.

(xxiii) Should able to generate reports on predefined / customized hours.

(xxiv) Highly Flexible Group based Reporting: It shall be possible to use a KPI at different network element levels (individual Network Device, Interface, Group of Network Devices, Links, etc.) and time dimensions out of the box modifying the KPI definition.

(xxv) The system must support complex KPIs that are constructed by weighted combination of other KPIs.

(xxvi) Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.

(xxvii) It should be able to generate SLA Reports on Availability & Performance

(xxviii) Should create historical performance and trend analysis for capacity planning.

(xxix) Should have capability to exclude the planned-downtimes or downtime outside SLA.

(d) **Centralized ITIL Aligned IT Service Desk:**

(i) The proposed Service Desk will be one of the most essential components of Network Operations Center. It will be the central mechanism for NOC staff to track and respond to requests and problems logged by end users and also work upon other NOC functions such as Change Management, Knowledge Management, Release Management, etc. Thus, it is expected that the proposed Service Desk is well aligned to maximum number of ITIL processes such as:

a. Incident Management
b. Request Fulfillment
c. Problem Management
d. Change Management
e. Release & Deployment Management
f. Knowledge Management
g. Service Asset & Configuration Management
h. Service Catalog Management
i. Service Level Management
j. Service Portfolio Management
k. Availability Management
l. Capacity Management
m. Event Management

n. Financial Management
o. IT Service Continuity Management

(ii) General Requirements of Service Desk

a. Should able to support and handle large volume of incidents
b. Should able to support and handle large volume of service requests
c. Should able to support and handle large volume of changes
d. Native integration of processes i.e. Incident Management with Change Management and vice-versa
e. Native integration of processes with Knowledge base i.e. automatically creation of knowledge base post closure of tickets
f. The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB
g. Able to create and modify forms as per GoG/DST requirement
h. Able to define different SLAs for different services / domains
i. Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units
j. Able to define different workflows for different processes
k. Able to send automatic escalation mails as defined in workflow
l. Should be able to integrate CMDB from different federated data sources and build a single CMDB
m. Should provide email based interactions allowing ticket creation, update and approval of request.
n. Should able to integrate with Active Directory and populate user information automatically
o. The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.
p. The system should have graphical interface to define, visualize and update ITIL processes

(iii) Service Catalogue Functionality

a. Should support single service catalogue for end users to submit and track service request, spanning ALL IT services

b. Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT services

c. Various types of Customer profiles should be supported such as, for ex: Profile-1: CMO, Profile-2: IAS Cadre, Profile-3: Grade 2 Officers and so on.

d. Integrates with any underlying service management including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment

e. Should have catalogues that cover standard and non-standard IT services

f. The services should be integrated to SLAs and should be auto measured for adherence.

g. The solution should have out of box catalogue for common request like IMAC, configure mail box etc.

h. Users should be able to request for services on behalf of other employees and the system should track the request as if the request has been initiated by the user requesting for the service.

(iv) Service / Help Desk (Incident and Problem Management)

a. Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT services that shall span across multiple domains like GSWAN, GSDC etc.

b. Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.

c. The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations

d. It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively

e. Solution should support fast service restoration leveraging previous incident data.

f. It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.

g. It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

h. Should support full text search capabilities

i. Should centralize all known error and problem workarounds into a single, searchable knowledge base

j. The incident Management solution should be completely integrated to the CMDB to ensure that CIs can be associated with the ticket to provide better visibility

k. The incident management solution should have the ability to initiate the change request on a button click

l. The solution should have the ability to associate an incident with an existing change request, a problem or known error for tracking purposes

m. It should allow the CI to be associated with tickets.

(v) Change & Release Management

a. The solution should be able to track a request for change through the different stages of lifecycle of a change request

b. The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency

c. The tool should facilitate the differentiation of normal Changes For example: Category - Minor or Small, Category - Significant or Medium, Category – Major or Large

d. The tool should facilitate the ability to create simple to complex request workflows through sequential and parallel tasking

e. The tool should notify all the users about the scheduled changes/outage and sent a reminder to responsible contacts

for implementation of change

f. Change management should have fields to record impact analysis and simulate impact, back-out plans, within the change record

g. It should have the capability to automatically and continually perform impact analysis, risk assessment, and change collision dates detection (for same CI's) on all change requests. The solution should provide complete view of planned changes with services & their components.

h. The tool should facilitate the scheduling of post implementation reviews for implemented changes after defined time interval

i. The application should have the ability to assign change advisory board (CAB) responsibilities to change management roles

j. The tool should facilitate ability of authorized roles to reject changes For example, status of reject, ability to record reason for rejects notification

k. The change approval engine should be configurable such that approvals can happen if either one of the individuals approves a change, or a majority approve the change, or certain people in the committee approve the change etc. It should also incorporate multi-staged approvals like MD-GIL, JS-IT, Sec-IT etc.

l. Change management should be capable of integrating with CMDB to facilitate access to CI attributes and relationships to enable change assessment and authorization

m. The solution should allow the identification of post implementation impact and resource utilization for completed changes, track incidents and problems resulting from an implemented change, further enable analysis of planned versus actual resources utilized for change

n. Solution should provide a consolidated view of the tasks that the release management team must perform to drive the completion of the change requests and activities required to close the release.

o. Solution should provide Change and Release Calendar views for the current schedule of releases, change requests, and business events for any potential conflicts.

p. Solution should provide the ability to analyse the impact of change to the appropriate business services and IT services.

q. The solution should have the ability to prompt change planners with suitable time slots for conducting a change depending upon the changes that have been scheduled/in progress, risk associated with it and the priority of the change.

r. The solution should have the ability to identifying and flagging changes that are being done by various team to prevent change collisions.

(vi) Knowledge Management

a. The tool should have the knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions

b. The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system

c. The tool should allow creation and enforced use of data input rules for creating knowledge records For example: mandatory fields for content and information; QA and change approval to move from draft to production

d. The tool should allow for the entry of free-form text, images, attachments, etc.

e. The tool should automate the population of knowledge records with author and owner data, creation date, as well as any other attributes required by organization

f. The tool should facilitate the identification of redundant or duplicate information, whether in single record or multiple records

g. The tool should allow automating notification to interested parties on submission new knowledge/solutions applicable to them

h. The tool should have a powerful search engine to sort, retrieve and search using advanced search options, search content in multiple format, and also search within knowledge records

i. The tool should allow displaying FAQs and highlight the newly added knowledge content

j. The module should allow integration with all other modules of service management to enable knowledge records to be quickly created from records with associated links.

k. The solution should have the ability to prompt users with interactive set of questions and answers that will eventually guide the users to the relevant solution.

l. The module will facilitate opening of a problem record directly from a menu for pro-active tracking of problem activity as well as from an incident record for reactive tracking of problem activity.

(vii) Configuration Management database (CMDB)

a. The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process

b. Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes

c. Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time

d. The proposed helpdesk solution must allow the IT team to see the CI relationships in pictorial format, with a specified number of relationships on single window.

e. The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc.

f. Should provide Attribute-level normalization and reconciliation to leverage existing data from third-party asset or discovery tools and realize the goal of having one dependable source of

configuration data.

(viii) Service level Management

a. Solution should support comprehensive SLA management platform

b. Manage service levels for delivery and support of business services

c. Must allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.

d. Real-time visualization of service level targets, agreement compliance data, penalties and rewards.

e. The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – ex. 'pending information from customer'

f. The SLM module should integrate with incident and problem management to automate escalation, and notification activities based on response and resolution targets

g. It should also integrate with change management to provide access to service level agreement details, implementation windows, change blackout periods, and availability requirements

h. The application should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s). It should contain predefined status codes and allow defining new status codes

i. The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure For example: IDs of individuals or groups opening, updating & closing records; dates / times of status & activities updates, etc.

(ix) Dashboard Reporting

a. The Solution should provide a centralized Dashboard that picks up relevant business metrics from the service management solution giving at-a-glance visibility to key operational

initiatives

b. GoG/DST assigned staff members should be able to graphically view the health of their business services and its related ticket KPI's pertaining to different categories and departments configured in Service Desk.

c. These dashboards need to be dynamic that allows user to drag and drop these metrics and create custom dashboards without any coding.

d. The Dashboards should support rich formatting capabilities to represent the data in different chart formats.

(e) **Business Services Dashboard**

(i) Proposed Business Services Dashboard should provide flexible, role-based dashboards (for IT executives and service owners of GoG/DST) and operational consoles (for operations managers in NOC and technical staff) for a common understanding of service status, risks and quality problems. This should give the right experts actionable information so IT executives can focus operations on business priorities, service owners understand IT status in business terms, and operations staff always knows which components in their technology domains are impacting specific business services and can proactively mitigate risks.

(ii) The proposed Business Services Dashboard Solution must enable intelligent service modeling by importing IT components (like network devices, server resources, applications, transactions etc.) from the management tools that directly manage infrastructure and applications:

(iii) The Service Dashboard should display business service status in real-time. From the dashboard, operators should be able to launch technical operations console for service visualization, impact analysis, alert details and automated actions for remediation.

(iv) It should be possible to determine impact of network faults and performance degradation on customer services. .

(v) Solution should perform cross domain correlation between network alarms and degraded performance data received from multiple domains.

(vi) Solution should support capability to raise service problems for all the

impacted services. Solution should thus be able to indicate which network problems are end user service impacting and which are not. It should enable the categorization and prioritization of service problems.

(vii) The Business Process Views should have capability to provide business oriented views of the IT infrastructure management. For example, it should have capability to create views of the resources catering to GoG Departments who consume various IT Services of DST.

(f) **Service Level Management**

Service Level Management will be one of the crucial functions of Network Operations Center. SI's must propose a full fledge Service Level Management System that helps define, document, monitor, measure, report, and review the level of IT Services.

(i) SI's must proposed a full fledges Service Level Management Solution that allows for tracking of various service level performances of IT Infrastructure and vendor performance.

(ii) The product should be able to measure, collect, and import performance and SLA data from a wide range of sources, including performance Management modules

(iii) The SLM System should help to compute the automated weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the different agencies of RISL after applying the system of penalties and rewards as per the contract.

(iv) The solution should support SLA violations alerts during the tracking period.

(v) The solution should support the creation of different contracts which are currently underpinning with vendors.

(vi) The solution should support managing and maintaining a full history of an SLA.

(vii) Solution should support SLA violations in context of effective "impact" such as operational impact, financial impact and contractual impact.

(viii) The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators measured across infrastructure and vendors

(ix) The solution must have a unified repository to capture and manage all

service level templates.

(x) The solution must provide detailed control of the metrics that are being collected

(xi) The solution must contain out-of-the-box content for best practices frameworks such as ITIL.

(xii) The solution must support the concept of service templates, Service templates grouping and metric groupings.

(xiii) The solution must follow governance, compliance and content validations to improve standardization of service level contracts

(xiv) The solution must allow for grouping and composition of Services

(xv) The solution must have a pre-configured catalog of reusable Service Level Calculations and Aggregation methods.

(xvi) The solution provide document repository capabilities for supplemental documents associated with SLAs, SLA Management & Reporting process

(xvii) The solution must support management of service level agreement in a central repository.

(xviii) Creating of new service level agreements must be easy to be used by business and non-technical users.

(xix) The creation of SLA must be done via a Wizard driven interface

(xx) The solution must allow for customization of the service level agreement.

(xxi) The solution must have the ability to define and calculate key performance indicators (KPIs) from an End to End Business Service delivery perspective.

(xxii) The solution must support dependencies between business and technical metrics.

(xxiii) The solution must support dependencies between supplier's contracts and internal or external contracts.

(xxiv) The solution must support weighting of Service Level Indicators

(xxv) The solution must have the ability to manage multiple SLAs for the same contract party

(xxvi) Manage scheduled and un-scheduled maintenance windows

(xxvii) The solution must support SLA approval/validation workflow

(xxviii) The solution support role base access to service level agreements and sections in the service level agreements.

(xxix) Links to external or internal sources can be created from within service level agreements.

(xxx) Tight integration of SLA Creation & Reporting/Monitoring modules

(xxxi) The solution must support aggregation and correlation of performance data relatively to contractual agreements.

(xxxii) The solution must have an integrated dashboard

(xxxiii) View of Contract Parties & current SLA delivery levels

(xxxiv) View of Services & current SLA performance

(xxxv) he solution must support standard and user configurable aggregation

(xxxvi) The solution supports SLA Alerts escalation and approval process.

(xxxvii) The solution must make it possible to find the underlying events that cause the service level contract to fail.

(xxxviii) The solution must provide annotation capabilities that must appear in reports generated against the service level.

(xxxix) Provide pre-configured connectors and adapters

(xl) Timing for collection of data is configurable

(xli) Ability to define Adapters to data source in a visual manner without coding.

(xlii) Design, customize, & Generate reports easily & based on User Roles

(xliii) The system must include the ability to generate customer SLA document from SLA information entered in the solution

(xliv) The solution must allow for reporting across customers, Type of Customer, Business unit, Service, Product any configured area of measurement.

(xlv) Reports should be created in a friendly manner using visual tools and wizards without any code or database query configuration.

(xlvi) Report module and SLA Management module must be integrated to provide ease-of reports configuration and execution.

(xlvii) The solution must support data integrity in reports correlation and present the end users indication regarding reports which includes data manipulations, corrections and exceptions,

(xlviii) The solution must allow the distribution of reports to appropriate roles/people, through Web-based interface/ Web Portal, or via email

(xlix) The solution must support single sign-on as well as integrate LDAP for user login and authentication.

(f) Systems & Applications Monitoring

(i) The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems, Databases, and Web based Applications in GSDC

(ii) The Tool must be able to integrate with existing Systems and Applications Monitoring tool

(iii) The Tools must be able to measure systems availability and performance in near real time

(iv) The Solution offered should be highly scalable to be able to monitor hundreds of servers in datacenter

(v) The End user experience solution must be proposed to measure availability and response time of applications by end users in real time.

(vi) End user monitoring solution must monitor the availability and performance of applications over the network end to end without generating any additional traffic by means of passive monitoring of transactions.

(vii) The Systems and Applications monitoring solution must tightly integrate with other layers of proposed solutions such as Event Correlation Engine, Business Services Dashboard and Service Level Management solutions.

(viii) The Systems Monitoring solution must have robust performance reporting engine in order to do performance polling of metrics and provide trend and capacity based report on measured metrics.

(g) **IT Asset Management**

SI must propose an IT Asset Inventory Management Solution that shall enable centralized and automated management of IT assets governed from Central Site.

(i) Solution must be able to discovery IT Assets for Inventory Management Purposes

(ii) The discovered IT Assets must be maintained in a single IT Asset Repository database for better and single pane of glass visibility for all IT Assets

(iii) The discovery should have feature of scheduling the discovery at specific periods

(iv) The discovery solution or IT Asset Management solution should also

support IT Asset inventory import from other data sources such as excel inventory, monitoring tools like Network Monitoring tool for a holistic IT Asset Inventory collection.

(v) IT Asset Management solution must be able to integrate with proposed monitoring solutions to perform auto discover into Asset Management database.

(vi) Solution must be able to track Warranty / AMC of all IT Assets

(h) **Network Configuration Automation**

(i) The Network Monitoring Solution must also have Configuration Automation feature for the monitored devices

(ii) The system should be able to clearly identify configuration changes as root cause of network problems

(iii) The system should support secure device configuration capture and upload and thereby detect inconsistent "running" and "startup" configurations and alert the administrators.

(iv) The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:

a. Capture running configuration

b. Capture startup configuration

c. Upload configuration

d. Write startup configuration

e. Upload firmware

(v) The proposed fault management solution must able to perform "load & merge" configuration changes to multiple network devices

(vi) The proposed fault management solution must able to perform real-time or scheduled capture of device configurations

(vii) The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

2.6.3 Successful bidder shall provide the following

(a) NMS reports including Bandwidth utilization report & Link up-time report & network equipment health check report on a monthly basis.

(b) Change management carried out by Helpdesk operation.

(c) Network Device Performance Report for SC-DC-TC and other priority offices, Weekly Monthly.

(d) Change management report – Monthly

(e) New Location Connectivity –Weekly, Monthly

(f) Asset Report Location wise – Monthly

(g) Help Desk Report – Daily, Weekly , Monthly

(h) NetQOS Report about utilization of Network protocol and GOG applications.

(i) Vendor SLA Violation Report – Weekly , Monthly

(j) Audit Report – Quarterly

(k) Network Utilization Report – Monthly

(l) Network performance after Integration (with other network) Reports – every 6 month.

(m) VC & other Web Event completion report –Monthly

(n) Preventive Maintenance Report - Quarterly

2.6.4 Successful bidder shall have to consult DST/GIL for finalizing the report formats and frequency formulating a Communication Plan prior to the start of services. Successful bidder shall also enable the GoG designated Officer to be able to view any (up-to-date/ historical) reports related to GSWAN and GSDC at any point of time via a Web-based interface to the NMS.

2.6.5 Bidder should also provide on-line Dash board where, DST can get summary view of GSWAN and GSDC Connectivity and Health Status.

2.6.6 Successful bidder would generate and provide Reports as stated below periodically. Bidder shall also be under obligation to provide any other reports as asked by DST, GoG.

2.6.7 **General Reporting Features:**

(a) Shall be able to present the reports through web, and also generate "PDF" version reports of the same.

(b) Should provide user flexibility to create customized reports according to the user privilege level.

(c) Should provide information regarding capacity utilization and error statistics for physical and logical WAN links.

(d) Should create reports on trend analysis and capacity planning from historical data and also by considering Mean Time Between Failure (MTBF) of equipment.

(e) Should be capable to send the reports through e-mail to predefined user at pre-defined interval.

(f) Should have capability to exclude the planned downtimes from SLA.

(g) Should be able to generate web based reports both in near real time and historical data for supported devices.

2.6.8 **Availability Reports**

(a) Overall Network Availability and Uptime Report on Daily, Weekly, Monthly, Yearly basis through GUI.

(b) Uptime & Availability Report for Vendor/Service provider; MPLS network, Leased Lines, LAN, Server on Daily, Weekly, Monthly, Yearly basis.

(c) Uptime & Availability Report on Network Devices: Router, Switch, Security Appliance on Daily, Weekly, Monthly, Yearly basis.

(d) Uptime & Availability Report of UPS at State, District & Taluka level on Daily, Weekly, Monthly, Yearly basis.

(e) Mean Time To Acknowledge (MTTA) and Mean Time To Repair (MTTR) Reports.

2.6.9 **Performance Reports**

(a) Overall Network Device Performance (Router, Switch, Security Appliance) – CPU and Memory Utilized at State, District & Taluka level.

(b) Every Link Input/Output Utilization (percentage, bps, kbps, mbps, octets/sec) on Leased Line, Wireless, Trunks between Switches, Link errors (Leased Lines, ISDN, Trunks, etc).

(c) Should be able to indicate the Network Latency, Flapping Links, Changed Link Metrics, Prefix List and New Prefixes on each leased links at State, District & Taluka level.

(d) Trend report based on Historical Information.

2.6.10 **SLA Based Report:**

(a) Should be able to do computation of SLA for entire GSWAN network and Individual links

(b) Should be able to generate automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports

(c) Should be able to present "At-a-Glance" report comprising critical SLA parameters

(d) Should provide component level report.

2.6.11 **Inventory Status Report:**

(a) Equipment Inventory report –device name, device part number & serial number, device model number deployed at SC, DC & TC level.

(b) Change Management report - Change management scorecards, change audit reports, changes by user and change detail reports provide immediate visibility into whether or not the defined CCM process is working and being followed.

2.6.12 **Event & Fault Management Report**

(a) Should provide details about the number of complaints received due to failure of network devices and Voice devices.

(b) Should provide the exact time and date when the complaints was resolved on daily, monthly and yearly basis. This should include the time taken to resolve the complaint and the reason due to which fault had occurred.

2.7 Quality of Service (QoS)

2.7.1 Successful bidder shall configure quality of service (QoS) parameters on network

switching and routing devices for end-to-end QoS for voice, video and other critical traffic over the network. Successful bidder shall configure network management policies for managing all the network and security devices using network management systems. Bidder will also be responsible for generating NETQOS reports from NMS tool and adhering to such policies that are issued from time to time by GoG.

2.8 Helpdesk / Contact Centre

2.8.1 For servicing the GSWAN users, Successful bidder will implement centralized Helpdesk System with IVR (Intelligent Voice Recognition), E-mail, SMS and Call-tracking mechanism. The Helpdesk would be operated by a Third Party vendor appointed by DST/GIL. The Helpdesk should allow GSWAN and GSDC users to log queries / complaints on a centralized phone number, which should be resolved as per the Service Level requirements. The helpdesk queries / complaints related to connectivity, security, configuration or any other issues which relate to the usage of GSWAN and GSDC should be handled by the Helpdesk. Daily report of calls logged and resolved should be generated and submitted to GoG. GoG would locate the Helpdesk Centre at a different location from NOC. Bidder shall be responsible to provide required hardware, Helpdesk Software and licenses to setup this Helpdesk. The Helpdesk software should be able to take care of classification, automatic escalation, management, status tracking and reporting of incidents as expected by the service level requirements. Status tracking should be available to GSWAN and GSDC users through the centralized Help Desk number as well as online through software. Helpdesk software should also give a report on status of calls and violation of SLAs during disposal of such calls. Bidder shall be responsible to provide training to the Call Centre Agents to use the Helpdesk Software. Bidder shall deploy one resource to coordinate with the Helpdesk team to assign priorities to tickets generated.

1.8.2 **Problem Resolution and Sign-Off**

GSWAN and GSDC users would report any network related problem through online Helpdesk interface or by calling the Centralized Helpdesk number. The severity of the call will be automatically decided according to the Helpdesk Severity Matrix detailed in the SLA section. The Bidder will keep track of Helpdesk performance. This online report

would contain:

(a) Trouble Ticket Number as generated in the Online System

(b) Time at which the problem was logged

(c) Problem Description

(d) Customer Details – Contact and Location

(e) Helpdesk Engineer

(f) Problem Resolution Time

(g) Cause of problem

1.8.3 At the end of each problem resolution performed by the Helpdesk or GSWAN Engineer at respective location, the GSWAN engineer would provide a confirmation by sending a ping to a designated IP form the end user desktop/laptop. The receipt of ping from the end user IP would automatically indicate closure of call.

2.9 Operation & services of horizontal links from all PoPs or otherwise.

2.9.1 Successful Bidder would be responsible for uptime as mentioned in SLA for defined district level and taluka level PoPs. The Bidder would be responsible for operation and services of horizontal links. This includes fault detection, analysis and escalation to respective agencies and DST/GIL within 4 hours of down-link reported in NMS tool or otherwise or on helpdesk and follow-up with respective agencies to close the complaint. Successful Bidder would be responsible for uptime as mentioned in the SLA for these existing approx. 5500 horizontal links at horizontal offices at SC, DC & TC as well as for new horizontal links which may be established during contract period at the unit rates specified in the bid.

2.10 Implementation, operations and services & maintenance of New PoPs

2.10.1 In case DST desires to set up the new PoPs, one-time cost for implementation/ setting up of new PoPs should be quoted by the bidder. After implementation of the said PoPs, Operation, Services and maintenance of new PoPs will be applicable at the quoted unit rate of operation, service and maintenance rate of other PoPs ,as defined in this bid .

2.10.2 At any time during the contract period, DST may ask successful bidder to create the

new PoPs as per the requirement. Bidder has to set up this new PoPs in consultation with DST. For any new PoPs set up/implementation, all equipments (including Routers/switches/UPS/ and required accessories/consumables (I/O/ UTP cable, PVC Pipe, & necessary electrification including switch and plug) would be procured/ supplied by DST, GOG. Link commissioning/Termination and Bandwidth provisioning would be the responsibility of DST, GOG.

2.10.3 Implementation activity would mainly constitute:

(a) Configuration of Network equipment i.e. Routers, Switch/Modem/Hub

(b) Liaison with service providers,

(c) Co-ordinate with NOC State Centre team of the bidder for checking connectivity related issue

(d) Discovery of New POP Location in Centralized NMS Tool

(e) Update of Asset Register after implementation of new POP

2.10.4 It is the responsibility of the successful bidder to maintain the networking infrastructure at the existing/newly created PoPs. All the networking equipment shall be kept in good working condition and shall be repaired or replaced. In case of any equipment which is under Warranty the Bidder would be required to liaise with respective Vendor to ensure that all equipments are repaired/ replaced.

2.10.5 All the electrical equipment and accessories including lighting equipment, backup power sources, plugs, wires etc. shall be maintained and if required replaced by the successful bidder at its own cost. The successful bidder shall deploy the prescribed resources as given in the proposed technical solution in the technical bid of RFP for ensuring desired uptime of all GSWAN PoPs and other IT infrastructure. At various PoPs, the bidder shall provide maintenance and support services.

2.10.6 The Successful bidder shall also maintain an up-to-date inventory of all GSWAN supported equipment and spares and make the same available for review and inspections every quarter by DST/GIL.

2.11 Operations & Maintenance of Gujarat State Data Centre (GSDC)

2.11.1 The scope of work to be undertaken by the bidder for Operations, Management and Comprehensive Annual Maintenance Contract (CAMC) of the IT & Non-IT Infrastructure for the Gujarat State Data Centre (GSDC) is mentioned below.

(a) The selected bidder shall be responsible for O&M of all IT and Non-IT Infrastructure installed in GSDC. The list of equipments installed in GSDC is placed as Annexure "G".

(b) The selected bidder shall ensure an uptime of 99.741% on quarterly basis for both IT and Non-IT Infrastructure components.

(c) Bidder must produce Standard Operating Procedures (SOPs), processes, Technical design/architecture, layouts/templates must be well documented for operating each IT and Non-IT Infrastructure components and should kept updated with most recent changes.

(d) The scope of work during the operations phase should cover but not limited to following areas:

(i) System, Servers, Storage, Database, Security and Network - Administration, Configuration, Hardening, Maintenance and Operations Management

(ii) Backup and Restore Services

(iii) Preventive and Corrective Maintenance

(iv) Asset Management Services

(v) Vendor Management Services

(vi) Email/Messaging Services

(vii) MIS Reports (monthly, quarterly or as and when asked by DST)

(viii) Implementation and Compliance of ISO Standards (27001:2013 and 20000). Bidder shall ensure the ISO Certification is kept current and updated during the Contract period without additional cost

(ix) Application and Website Hosting Management

(x) Patch Release Update management

(xi) Software (Operating System, Anti-Virus, Enterprise Management Suite, Spam & URL filter etc.) - Administration, Configuration, Hardening, Maintenance and Operations Management

(xii) Non-IT Infrastructure Management and Maintenance shall include equipment/components but not limited to Transformers, Circuit Breaker, DG Set, Electrical/Mechanical components, UPSs, battery banks, electrical cables, industrial sockets, Fire and Safety system, water leakage detection system, Building Management System (BMS), Surveillance systems (CCTV), Access control, Public Address System, Pest and rodent repellent system, Civil Infrastructure, Racks, Power Distribution Unit (PDUs), Precision Air Conditioners (PAC), False Ceiling and Data Centre Floor, etc. The detailed list of Non-IT Infrastructure Items is placed at Annexure "E".

(xiii) At present the Server and Storage Room is spread across 2600 Sq.ft. which is planned to be expanded to approximately 4000 Sq. ft. in near future. The additional 1400 Sq.ft. of the Server and Storage area would also come under the responsibility of the selected bidder for O&M purposes.

2.11.2 The scope of work is not only limited to currently deployed IT and Non-IT Infrastructure components at Gujarat State Data Centre but also includes O&M for any additional equipment/devices/hardware/software that is supposed to be deployed at SDC during the contract period of 5 years.

2.11.3 Agency will be responsible for O&M for any additional equipment /devices /hardware /software procured by DST and hosted at GSDC, 1% of the cost for each additional equipment/devices/hardware/software component, per annum would be applicable for additional payment as part of O&M and SLA of 99.741% uptime will be enforced on new equipment /devices /hardware /software.

2.11.4 Following services shall be provided by the O&M agency under the basic infrastructure services, but not limited to the following:

(a) Ensure availability (99.741%) of the SDC IT infrastructure

(b) Facilitate hosting of departmental application, websites and infrastructure at the SDC:

(i) Provide testing / staging facility on existing and new infrastructure for testing the application infrastructure before hosting on the racks.

(ii) Ensure availability of the other peripheral infrastructure such as SAN, network etc.

(iii) Ensure the connectivity between GSWAN and SDC devices.

(c) Ensure proactive maintenance of IT Infrastructure components and repair or replacement of defective IT Infrastructure components deployed at the SDC which is under valid AMC contract.

(d) DST/GIL may procure necessary software licenses as required from time to time and the same shall be implemented, customized and managed by the O&M agency.

(e) Any IT component (for the devices whose AMC is included) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA). The selected bidder shall ensure that the uptime commitment as per SLA is met.

2.12 IT Infrastructure Security Administration

2.12.1 The activities to be carried out under security administration shall include, but not limited to the following:

(a) Addressing the ongoing needs of Security Management including, Monitoring and Management of various devices / tools such as Firewall, SIEM Tool, Intrusion Prevention System, Content Filtering and URL Blocking, Virus Protection, Load Balancer, DMZs, VLANs, Proxy and vulnerability protection through implementation of proper patches and rules as per best practices.

(b) Carrying out periodic Vulnerability Analysis and Penetration Testing (VAPT) to ensure that SDC systems and network are safe and secure.

(c) Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.

(d) Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

(e) Respond to security breaches or other security incidents and ensure that workaround / patches are made available for the same.

(f) Provide a well-designed access management system, security of physical and digital IT assets, data and network security, backup and recovery etc.

(g) Maintenance and management of IT security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.

(h) Ensuring that the IT security policy is maintained and updates to the same are made regularly as per ISO 27001:2013, ISO 20000 guidelines.

(i) Access Control Management

(i) Audit Trail and Log Analysis
(ii) Establishing and monitoring access control

(j) Firewall policy management which will include the Configuration & Patch Management Intrusion Detection System Management: This arrangement shall include Incident Handling and recovery. The Incident Handling Procedure (IHP) has to be followed as per the guidelines drawn by the DST, GoG. This would also include virus and spam control, policy configuration & management. The audit logs shall be maintained by the Bidder for review. The bidder would also establish counter measures that are needed for the perceived risks. The bidder shall establish the counter measures to mitigate the risk.

2.13 Vendor Management Services

2.13.1 The activities shall include, but not limited to the following:

(a) O&M agency shall coordinate and follow-up with all the relevant vendors of the State User Department to ensure that the user problems and issues are resolved in accordance with the SLAs agreed upon with them by updating the GIL / DST, GOG as and when deviation in the SLA is reported.

(b) O&M agency shall also ensure that unresolved issues are escalated to respective user departments / GIL / DST, GOG in accordance with the escalation matrix.

(c) O&M agency shall also coordinate with Chief Information Officers (CIOs) / Officers designated by the User Departments who would host their IT infrastructure at the SDC and ensure that the issues are resolved in accordance with the SLA signed between the User Departments and their vendors/ Application Developers. O&M agency shall maintain a track of SLA performance for such vendors.

(d) O&M agency shall maintain database of the CIOs / designated officers and various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.

(e) O&M agency shall draw a consolidated quarterly SLA performance report as defined by the GIL / DST, GOG / Departments across vendors for consideration of the user departments. (Monthly & Quarterly - Common for GSDC and GSWAN)

2.14 License Management

2.14.1 The activities shall include, but not limited to the following:

(a) All the software licenses should be in the name of Government of Gujarat.

(b) O&M agency shall keep the record of all the software licenses and track software usage throughout the IT setup so as to effectively manage the risk of effective usage of software installed at the SDC.

(c) The O&M agency shall avoid the unauthorized usage of Licensed Software. In the event of any claim asserted by Third Party of Infringement of Copyright, Patent or Trademark arising from the use of IT components or software, the O&M agency shall be entirely responsible to extinguish such a claim. If the O&M agency fails to comply and the DST, GOG is required to pay the compensation to the Third Party resulting from such infringement, the O&M agency shall be responsible for the compensation including all expenses, court costs and lawyer fees.

2.15 Email/Messaging Services

2.15.1 The activities shall include, but not limited to the following:

(a) End-to-end management of messaging systems

(b) Administration of mail servers

(c) Monitoring performance and management of user accounts, mail boxes, post office and address book.

(d) Backup and archival management.

(e) Transaction log management.

(f) Implementation of mail policies as defined by the State and in accordance with the prevailing Cyber laws , including, user security, access control, encryption, mail box sizes, mail sizes, spam, content filtering, etc.

(g) Management and monitoring mail queues, mail routing of incoming and outgoing Internet mail.

(h) The O&M agency shall be responsible for

(i) Maintaining the messaging application and individual mailboxes,

(ii) Adding / removing Mail IDs with permission from DST.

(iii) Troubleshooting any problems in the messaging system and messaging client.

(iv) Monitoring the mailbox usage.

(v) Ensuring timely delivery of mails.

(vi) Keeping a track on the mails getting dropped and taking backups of the mailboxes at regular intervals.

(vii) Purging and compaction of mail boxes at regular intervals for optimum utilization of resources as per the policies.

(viii) Monitoring the performance statistics including mail server utilization statistics, memory management, CPU utilization and disk space utilization according to the Service level agreement.

(ix) Deployment of SPAM filter and monitoring mechanism.

(x) Maintaining and troubleshooting spam/content filter applications

(xi) Regular updation of Blacklist / whitelist and manual spam filter rules.

(xii) Operate and Manage Gateway Level content filtering / mining mechanism,

(xiii) Prepare log report from Messaging system including Anti-Spam and Content Filtering for reporting the incidents of SPAM mails, Virus Mails and Accessing the restricted sites/contents. The report to be submitted to DST/GIL on periodic basis for review and taking corrective actions.

(xiv) Manage gateway level SMTP antivirus and Anti-spam solution.

(xv) Security and Maintaining Confidentiality, Integrity and Availability of the E-Mail Data and Services.

(xvi) All incoming and outgoing mail traffic shall be routed through gateway anti-virus and checked/ verified to be malicious content free.

2.16 Server Administration and Management Services

2.16.1 The activities shall include, but not limited to the following:

(a) Installation and Configuration of server, Hardware & OS parameters, operating systems administration and tuning.

(b) Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of upgrades including migration to higher versions and patches to ensure that the system is properly updated.

(c) Installation/Re-installation of the Operating System for newly procured hardware/software licenses or in the event of system crash/failures.

(d) Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.

(e) Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. Ensuring that the logs are backed up and truncated at regular intervals.

(f) Periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

(g) Ensuring the upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract.

(h) Troubleshooting issues in the infrastructure, network and applications to determine the areas where fixes are required and ensuring resolution of the same.

(i) Identification, diagnosis and resolution of problem areas pertaining to the SDC's IT Infrastructure and application and maintenance of assured SLA levels.

(j) Implementation and maintenance of standard operating procedures for maintenance of the IT infrastructure based on the State's policies.

(k) Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.

(l) System administration activities shall include tasks including but not limited to setting up the servers, executing hardware upgrades, hardening and software updates when necessary

(m) Recommend required preventive maintenance plan to the GIL / DST, GOG and should prepare schedule accordingly.

(n) Necessary information as and when requested by the GIL / DST, GOG.

(o) Coordination with the GIL / DST, GOG for smooth functioning of the services.

2.17 Storage Administration and Management Services

2.17.1 The activities shall include, but not limited to the following:

(a) Configuration of the storage system at SDC.

(b) Management of storage environment to maintain performance at desired optimum levels.

(c) Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, VTL etc.

(d) Configuration of SAN whenever a new application is hosted on the SDC. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.

2.18 Backup and Restore Services

1.18.1 The activities shall include, but not limited to the following:

(a) Backup of database and application as per stipulated policies at the SDC.

(b) The backup of necessary data/information will be carried out by the O&M agency in consultation with DST/GIL. The backup schedule like daily, weekly, monthly should be designed and implemented by the Bidder. Bidder will have to submit these backup reports periodically to the DST/GIL.

(c) Ensuring prompt execution of on-demand backups/restoration of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system.

(d) Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.

(e) Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.

(f) Physical security of the media stored in fire resistant cabinets

(g) Drill activity for the backup and restore to be done by the O&M agency. The application vendor will provide the assistance to the O&M agency as and when required regarding the drill activity and the O&M agency would be responsible to take the back up in concurrence with the application vendor and GIL / GoG in accordance with the defined back up policy.

(h) Off-Site backup of the database and the applications as per stipulated policies shall be carried out by the O&M agency for SDC.

2.19 Installation and Configuration of Application Infrastructure

1.19.1 O&M agency shall provide installation and configuration support for the application infrastructure to be hosted by User Departments. The activities shall include, but not

limited to the following:

(a) O&M agency shall undertake pre-installation planning at the State Data Centre.

(b) O&M agency shall be responsible for co-ordination during the commissioning of the storage, network & security components and related basic infrastructure at the SDC.

(c) O&M agency shall carry out the planning and layout design for the placement of equipment in the SDC in consultation with the existing Implementation Partner. The plan and layout design should be developed in a manner so as to optimally and efficiently use the resources and facilities being provisioned at SDC.

(d) The plan and design documents for the departmental application servers, thus developed shall be submitted to the user departments for approval and the acceptance would be obtained prior to commencement of installation.

(e) The O&M Agency shall carry out Server, OS, Application, Database & Services Hardening as per Best Practices and GSDC Guidelines. The O&M Agency shall also check & verify that the Application Infrastructure (both Hardware and Software) is in compliance with GSDC's policy, process & procedures/Guidelines.

2.20 Integration Testing

1.20.1 This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the SDC operations and affect other infrastructure in terms of performance and security. The technical tasks to be carried out shall include, but not limited to the following:

(a) Functional Testing: Ensuring that the application functionality as described by the department works adequately on the SDC environment.

(b) Performance Testing: Ensuring that the application meets expressed performance requirements on the SDC servers by using performance test tools and performance monitoring tools

(c) Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure

2.21 MIS Reports

1.21.1 O&M agency shall submit the reports on a regular basis in a mutually decided format. The following is only an indicative list of MIS reports that may be submitted to the DST/GIL:

(a) Daily reports

(i) Summary of issues / complaints logged at the Help Desk

(ii) Summary of resolved, unresolved and escalated issues / complaints

(iii) Summary of resolved, unresolved and escalated issues / complaints to vendors.

(iv) Log of backup and restoration undertaken.

(v) Security Incidents

(vi) Component wise Report (Server, Network, Security devices, Backup, Website Updation, etc.)

(b) Weekly Reports

(i) Issues / Complaints Analysis report for virus calls, call trend, call history, etc.

(ii) Summary of systems rebooted.

(iii) Summary of issues / complaints logged with the OEMs.

(iv) Security Incidents

(v) Inventory of spare parts in the SDC.

(vi) Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

(c) Monthly reports

(i) Component wise IT infrastructure availability and resource utilization

(ii) Consolidated SLA / (non)-conformance report.

(iii) Summary of component wise Data Centre uptime.

(iv) Summary of changes in the Data Centre.

(v) Security Incidents

(vi) Log of preventive / scheduled maintenance undertaken

(vii) Log of break-fix maintenance undertaken.

(d) Quarterly Reports

(i) Consolidated component-wise Non-IT and IT infrastructure availability and resource utilization.

(e) Half-yearly Reports

(i) Data Centre Security Audit Report

(ii) IT infrastructure Upgrade / Obsolescence Report

(iii) Risk Assessment, Risk Management and Risk treatment Report

(f) Incident Reporting

(i) Detection of security vulnerability with the available solutions / workarounds for fixing.

(ii) DoS attacks, Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.

(iii) Software license violations.

(g) MIS for reporting Attendance

(i) O&M agency has to report attendance on monthly basis.

(h) MIS reports related to Application Enhancements

(i) The O&M agency shall submit the following indicative list of deliverables for any change request, application enhancement.

(j) Impact Analysis Document

(k) Estimation of efforts with basis of estimation and breakup of estimation

(l) Tentative Project schedule

(m) Code coverage results

(n) Unit Test cases & results along with Defect Statistics

(o) System Test Plan, Cases & results (STS, STR) along with Defect Statistics

(p) Integration Test Cases & results along with Defect Statistics.

(q) Performance Test Report and Performance Tuning Report

(r) User Training Manual

(s) Traceability Matrix

(t) List of common errors and resolutions

2.22 ISO 27001 ISMS Standards for GSDC

2.22.1 O&M agency is responsible for maintaining the overall Information Security posture at GSDC. The O&M agency would be responsible for establishing, operating, monitoring, reviewing, maintaining and continuously improving the Information Security Management System (ISMS) at the SDC. The O&M agency shall be responsible for the implementation, sustenance of ISO/IEC 27000 standard and subsequent renewals/upgrades to ISO 27000 certification from the certification body such as STQC, BSI, DNV, BVQi, etc.

2.22.2 The regular revision/review/change of Policy, process & procedure documents as and when required is the responsibility of the O&M Agency.

2.22.3 O&M agency has to take consent of DST, GoG in case of any changes required in policy manual or documentation.

2.22.4 O&M Agency has to carry out Risk Analysis to identify and assess potential risks that could affect continuity of businesses at GSDC. O & M Agency will also be responsible to recommend and implement adequate measures such as Risk Treatment to counter/mitigate, the risks identified.

2.22.5 O&M Agency will carry out testing and execution of Business Continuity Plan and Disaster Recovery Plan

2.22.6 O&M Agency will conduct Workshops and Training sessions for all GSDC stake holders to create awareness of ISMS implementation. GSDC stake owners will be made familiar with ISMS implementation and risk management approach selected for SDC.

2.22.7 O&M agency will be responsible to apply and maintain the ISO 27001 certification for the contract duration.

2.23 ISO 20000 ITIL (Information Technology Infrastructure Library) Standard for GSDC

2.23.1 ISO/IEC 20000 adoption in Gujarat SDC infrastructure helps in ascertaining that the Services delivered to the GIL / DST, GOG / User Departments by the O&M agency are:

(a) As per the agreed Service levels

(b) Professionally managed with domain expertise

(c) Project Risks are well understood and managed

2.23.2 O&M agency shall be responsible to implement ISO/IEC 20000 standard which shall

promote the adoption of an integrated process approach to effectively deliver managed services to meet the SDC, GIL / DST, GOG and User Departments.

2.23.3 **Following methodologies are proposed for ITSM/ITIL standard:** PDCA (Plan-Do-Check-Act) methodology shall be adopted to implement ISO 20000 standard to establish the objectives and processes necessary to deliver results in accordance with GIL / DST, GOG requirements as well as the SDC policies and to implement the processes accordingly. O&M agency shall monitor and measure processes and services against policies objectives and requirements and report the results and take actions on the differences and continually improve process performance.

2.23.4 Alignment of information technology services and strategy.

2.23.5 To create a formal framework for current service improvement projects.

2.23.6 To improve relationship between different departments via better definitions & more clarity in terms of responsibility and goals.

2.23.7 To create stable framework for both resource training and service management automation.

2.24 Database Administration & Management Services

2.24.1 The activities shall include, but not limited to the following:

(a) End-to-end management of database on an ongoing basis to ensure smooth functioning of the same.

(b) Management of changes to database schema, disk space, storage, user roles.

(c) Conduct code and configuration reviews to provide tuning inputs to the State / User Department in order to improve the application performance or resolve bottlenecks if any.

(d) Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.

(e) Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.

(f) Continuous monitoring and periodic review of Database Logs, to identify performance bottlenecks, suspicious activities, signs of compromise, etc.

(g) Use of DBA tools related to performing database creation, maintenance, and database monitoring tasks.

2.25 Change Management

2.25.1 The activities shall include the following, but not limited to the following:

(a) Tracking the changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc.

(b) Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.

(c) Any changes (as and when required) at the architecture or configuration level for GSDC related components is part of the O&M activity and it should be carried out by the O&M Agency.

2.26 Application Related Services

2.26.1 The Information in this clause shall govern the methodology by which Application Related Services shall be provided to the State Data Centre at Gandhinagar.

2.26.2 Application related services shall complete the entire spectrum of services to be provided by the O&M agency. The objective of application related services is to facilitate the user departments by providing them with “One Stop Shop” for their requirements. As a part of these services, the O&M agency shall provide support for bug fixes, enhancements, operational support, and assistance to the User Department. These services have been classified under the following three categories depending upon the extent of application support that may be required by the User Departments:

(a) Application Monitoring and troubleshooting

(b) Website and Application hosting and management

(c) Application Enhancement

(d) Application Migration

2.26.3 The application hosted at the SDC will require management in the functionalities which includes, but not limited to the following:

(a) Monitor the departmental applications on a day-to-day basis to ensure that the application functions reliably.

(b) Monitor application to ensure that the application does not suspend, hang etc.

(c) Monitor components, including but not limited to, Application servers, Web Servers, Middleware and other application servers on an ongoing basis to ensure smooth functioning of the applications.

(d) Ability to troubleshoot problems, monitor erratic behavior through the application logs. Further, the O&M agency shall co-ordinate with application vendor for resolution of application related issues.

2.26.4 Coordinate with the application vendor to manage patch upgrade as and when required with minimal downtime. Ensure configuration management and backups of patch to rollback in case of problems.

2.28 O&M of Physical Infrastructure

1.28.1 All the devices installed as part of the physical infrastructure should be remotely monitored and managed on a 24x7x365 basis. The physical infrastructure management and maintenance services shall include, but not limited to the following:

(a) Operation and management of Building Management System. Proactive monitoring of the entire Physical infrastructure installed at through Building Management Software. Current BMS tool may be upgraded/replaced.

(b) Management of Physical Access to the premises as per the policies set by the Department of Science and Technology.

(c) Monitoring, recording and reporting usual and unusual movements in and around the premises.

(d) Material inward/ outward control as per policies set by the Department of Science and Technology.

(e) Monitoring and managing safety and surveillance equipment like CCTV, Access Control, Fire detection and Suppression etc.

(f) Issuing access control as per approval from the Department of Science and Technology.

(g) Reporting incidents to the Department of Science and Technology.

(h) Co-ordinate with respective trusted personnel and communicate with authorized maintenance personnel for various utilities at the Data Centre as required.

(i) Manage and monitor Diesel level/ requirements at its full capacity of the DG Set. Prevent the contamination of diesel by diesel bug or any other microorganisms. Diesel is consumable item, which will be charged on actual basis.

(j) Vendor Co-ordination for various physical Infrastructure components

(k) The bidder shall install a mechanism which will generate logs for diesel consumed through the use of tamper proof automatic measurement.

(l) Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent or higher configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.

(m) The selected bidder shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by DST/GIL or authorized authority.

(n) CCTV footage is to be kept to meet legal, regulatory, ISO Policies compliance requirements. The record retention period shall be as per policies of DST/GIL. New CCTV system shall be compatible with current SAN.

(o) The bidder should ensure high availability for power on 24x7x365 basis and should maintain all the systems/subsystems for power availability.(The detailed SLA is attached)

(p) Ensure availability of the physical Infrastructure including Power, Cooling, CCTV, Access Control, Intelligent Racks, Fire detection and suppression systems, Rodent Repellent systems, Water leak Detection Systems and other components included as part of physical Infrastructure related services.

(q) O&M AGENCY will have to submit monthly / quarterly MIS reports of each components as per the SLA

(r) O&M AGENCY should log SR / Incidents calls in service desk related to each component.

(s) Proactive and reactive maintenance, repair or replacement of defective components (IT and Non-IT/ Hardware and Software) related to Physical Infrastructure systems and sub-systems. The cost of repair and replacement shall be borne by the selected bidder. IT and Non-IT hardware here refers to systems such as IT and non-IT hardware and software being used for maintaining and monitoring Physical Infrastructure e.g. BMS, Access control, etc.

(t) The selected bidder shall have back-to-back arrangement with the OEMs and shall provide a copy of the service level agreement signed with respective OEMs.

(u) The Bidder shall maintain documentation for installation, testing, commissioning of any system/sub-systems that is installed or upgraded.

(v) Acceptance test shall be carried out for any system that is installed and/or upgraded.

(w) The bidder shall carry out comprehensive fire drills as per Policy/Guidelines specified by DST and submit drill reports to DST/GIL on regular intervals.

(x) Bidder shall record all the incidents/issues related to physical infrastructure services, security, systems and Sub-systems in the Helpdesk.

(y) The bidder shall carry out Risk assessment of the Physical Infrastructure as per Policy/Guidelines specified by DST and provide a Risk Assessment report including recommendations. Assessments/Policies/Guidelines defined are based on ISO 27001 and ISO 20000 Standards.

(z) The bidder shall provide training to resources deployed at periodically.

(aa) The bidder shall carry out current state assessment on an annual basis to determine the state of all the components installed and maintained, on completion the bidder shall submit a recommendation/up gradation report.

(bb) Full compliance to all the policies, procedures, processes, guidelines, Government- Acts, Rules & Regulations, etc. The bidder shall provide full compliance/adherence of all activities performed by them, to the aforementioned statutes, without any additional cost to DST/GIL.

(cc) Upgrading/Replacement of Current CCTV System with IP base Cameras with high resolution and night vision cameras. The O&M Agency is responsible for the integration of the Cameras with the NVR/DVR and ensure that at least 30 days 720p HD CCTV Footage is stored on the NVR and backup of CCTV footage beyond 30 days should be taken existing SAN/Tape Library, of GSDC. The bidder should ensure that the supplied CCTV system is compatible with existing SAN/Tape Library of GSDC.

1.28.2 Transformer, Circuit Breaker, Electricity and DG Set Maintenance & Management:

i) The O&M agency shall be responsible for Operations, Management and Comprehensive Annual Maintenance of Transformer, Circuit Breaker, HT/LT Power Cables, Electricity and Diesel Management for the entire project period. The O&M agency shall ensure that diesel shall be there in the DG sets at its full capacity in case of power failure. O&M agency has to maintain register for monitoring and reimbursing the diesel consumption for the DG set.

ii) Procedure for monitoring and reimbursing the Diesel consumption for the DG set:

(a) There will be a register maintained and kept with the O&M agency showing the following columns:

Sr. No	Date	Current Reading	Fuel Available	Date of filling	Qty Filled	Total fuel available	Signature of DST, GoG designated	Signature of O&M agency
1								
2								

(b) Reimbursement of diesel cost will be done on Quarterly basis along with Quarterly Payment.

(c) DST, GoG shall verify the diesel consumption from the log book maintained and MIS generated.

(d) The O&M agency will submit the bill (original bills of petrol/diesel pump) for every purchase along with their invoice for reimbursement.

(e) Payment will be processed by DST, GoG based upon verification of bill with the register entry on quarterly basis.

2.29 Preventive Maintenance Services

(a) Check, Repair/Replace any loose contacts in the cables/connectors & connections on a regular basis.

(b) Conduct preventive maintenance every three months or as directed by the DST, GoG (including inspection, testing, satisfactory execution of diagnostics and necessary repairing of the equipment).

(c) Cleaning and removal of dust, dirt etc. from the interior and exterior of the equipment on a daily basis.

(d) Preventive Maintenance Activities of components as per their manufactures' recommendation/advice.

(e) The Data Centre operator will keep a web based monitoring format and schedule of preventive maintenance services and shall provide reports to the DST, GoG as and when asked.

(f) The Preventive Maintenance shall be carried out in Non-Prime Hours only under prior intimation and approval from DST/GIL.

2.30 Corrective Maintenance Services

(a) Warranty and maintenance/troubleshooting of hardware problem of all supplied IT Infrastructure including network (active/passive) equipment, Security, etc. and support infrastructure equipment UPS, AC, DG Set etc. and rectification of the same.

(b) Troubleshooting of problems arising in the network and resolving the same.

(c) Documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems.

2.31 Asset Management Services

(a) The O&M agency shall be required to create database of all the equipments/software procured/Installed under Project. The details of all assets like hardware, software, peripherals, manuals, media and other related peripherals, etc., shall be maintained by recording information like make, model, configuration details, serial numbers, licensing agreements, warranty, place of installation etc.

(b) Record installation and removal of any equipment under the project and inform DST/GIL even if it is temporary.

(c) Create Software details with information such as Licenses, Version Numbers and Registration Details.

(d) Perform software license management, notify DST/GIL on licensing contract renewal and assist them in getting the license renewed.

(e) Asset Management services of physical and IT infrastructure under the project must conform to ITIL framework.

2.32 Configuration/Reconfiguration Management Services

(a) The successful bidder shall maintain complete configuration including reconfiguration (in & soft form in safe environment) for all equipment and handover the same to the DST/GIL at the time of completion of project or as and when asked by the DST/GIL.

(b) The O&M agency shall define and adhere to the change management procedures and also ensure that no unauthorized changes are carried out. Any changes shall be incorporated with prior approval of the DST/GIL.

(c) The O&M agency shall do proper version management of these configurations as they are bound to change from time to time.

(d) These configurations shall not be accessible in general and must be kept confidential.

2.33 Resource Requirement for Operation, Services and Maintenance

2.33.1 The minimum requirement of manpower resources, their qualification and responsibility of each resource is given below. This is minimum indicative list of

resources and based on actual requirements, the bidder may deploy any number of resources to meet the SLA. DST/GIL shall not pay any cost for additional resources required to operate, maintain, monitor & manage the GSDC & GSWAN as per the SLA. In case support staff is not available or is on leave, the bidder is required to provide the alternative personnel with same or higher technical capabilities of the non-available personnel..

S.No	Description	Qty	Roles & Responsibilities
1	State IT Infrastructure Project Manager	1	• Overall in-charge of O&M of the IT Infrastructure in SWAN and SDC. • Coordinating with third party agencies, bandwidth operators and software/equipment's vendors. • Should be the single point contact (SPOC) for managerial responsibilities and direct interface with DST/GIL.
2	Technical Manager (SDC)	1	• Responsible for overall management of the Data Centre, user SLA commitments, performance, availability, response time, problem resolution. • Should be responsible for effective Resource management, System & Resource planning, based on business forecast
3	Technical Manager (SWAN)	1	• Responsible for Network Planning, Designing & Optimization. • Responsible for network availability from Data Centre till last mile user node • Liaison with various stakeholders / agencies & GoG Departments for GSWAN related issues etc. • Responsible for Network services across client departments and citizens of the State as per the agreed Service Levels.
4	Network Administrator	2	• Responsible for network uptime, performance and other related services. • Network monitoring and proactive network uptime maintenance. • Network management (routing), Router Configuration and Troubleshooting, upgradation, Link Performance Management of L3 and L2 Switch at Data Center and GSWAN Network on day to day basis. • Support administration, Change Management, Liaison with Bandwidth Provider officials and external vendors, bandwidth and facility management

5	Engineer - Network Security Infrastructure	1	• Responsible for Firewall Management, Intrusion Management, Antivirus & Patch Management, Security Management. • Responsible for Firewall Rules and Policies Management and Troubleshooting Implementing of NAT/PAT, SSH, signatures, etc. • Plan & Implement comprehensive security policies and practices for entire infrastructure. Signatures updating, blocking of unwanted traffic Antivirus updates, Patch updates, managing the network security on day to day basis. • Monitoring any flooding, DoS, Intrusion attempt in real time during the office hours
6	Security Analyst	1	• Penetration Testing, Manual Testing, Writing Custom Exploits/Scripts. • Expertise in understanding information security, incident response, intrusion detection and prevention • Expertise in Data & Traffic Analysis, Network (TCP/IP), UNIX, Windows, Linux. • Experience in using System Security/Vulnerability Scanners /Sniffers • Experience with operating SIEM tool
7	EMS Engineer	2 + 2	• The resource should be able to administrate and manage the existing EMS Tools (Refer Annexure for the detailed list of tools) / the new EMS tools which are supplied as a part of this RFP. • Managing Network operations using EMS tool. • Managing Network Monitoring. • Responsible for monitoring of adherence to defined SLA by vendors by making effective utilization of deployed EMS tools in GSDC and GSWAN.
8	Helpdesk Manager	1	• Logging of support calls, escalation of calls, recording of configuration items and service calls monitor and control the Service levels and underlying service quality Creating MIS reports for management purpose Managing and Supporting the Helpdesk System (tool) for day-to-day operations. • Required to do recommended modifications, additions, deletions in tool. Managing and operating Helpdesk tool issues as a Tool Specialist.

9	Engineer – Server Management	1	• Managing server infrastructure services for GSDC's System maintenance, storage, backup etc. • Responsible for system configuration, scalability, performance, load balancing, OS administration / management, troubleshooting & Debugging and monitoring of servers. • Implement the back-up plan for storing and retrieving of data, maintain servers, machines, printers and also responsible in resolving the real time (RT) requests raised by users as per SLA. • Internet Management, E-Mail management, Service Management, End point solutions management, Systems Management, Proxy, content filtering and Internet access management for users, managing Messaging servers. • Monitoring application components, including Application servers, Web Servers, on an ongoing basis to ensure smooth functioning of the applications.
10	Engineer – Storage & Backup Management	1	• Backup of operating system, database and application as per stipulated policies at the SDC. • Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies. • Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by User Departments or in case of upgrades and configuration changes to the system. • Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes. • Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.
11	Database Administrator	1	• Responsible for database administration, should be responsible for database and application change management procedure. • Responsible for management of database repository, creation, deletion, modification, backup and restore of databases and their tables.

12	ISO Manager	1	• Management & compliance of ISO Policies, Process, Procedures and other applicable legislations, policies, guidelines…etc. • Carry out Documentation, technical report writing…etc. • Interface & co-ordinate with stakeholders for the Tickets raised in the Help Desk. • Should have very strong communication skills and technical writing skills. • Should possess working knowledge of ITIL, ISO 20000 & ISO 27001.
13	DR & BCP Engineer	1	• Define and develop RPO & RTO for each application, DB activities etc. • Document step by step technical DR strategy • Draft BCP process for identified critical applications • Run through mock drills of approved DR and BCP periodically after approval from DST/GIL • Adopt and develop DR and BCP guideline in line with ISO 22301 and other industry best practices • Should be able to manage DR Site components (hardware & software) • Co-ordinate between end-users and operation team for DR Testing & functioning
14	Video Conferencing Engineers	2	• Managing Video Conferencing events and equipments. • Vendor co-ordination and setting up of Video Conferencing sessions as per need and requirement.
15	Network Engineers (SCAN)	8	• Installation, troubleshooting, commissioning of network equipment for Sachivalaya Campus and horizontal offices in Gandhinagar. • Maintenance, Monitor and Support for network availability at the users end points in sachivalaya campus. • Installation, configuration and maintenance of wireless network in Sachivalaya Campus. • Regular update of software patches for network equipment, anti-virus etc.

16	Network Engineers (DC)	52	• Installation, Troubleshooting, commissioning of network equipment in District Control Room and horizontal offices at District level. • Maintenance, Monitor & Support for network equipment of POP. • Installation, configuration and maintenance of wireless network at District level. • Regular update of software patches for network equipment, antivirus etc. • Monitoring bandwidth utilization for the POP • Generating report and submit it to Project Manager (GSWAN). • Carry out and coordinate feasibility surveys for new connectivity in the district • Coordinate for VC events in DC Office and webcasting events in district
17	Network Engineers (TC)	248	• Installation, Troubleshooting, commissioning of network equipment in Taluka Centre and at horizontal offices at Taluka level. • Maintenance, Monitor & Support for network equipment of POP. • Installation, configuration and maintenance of wireless network at Taluka level. • Regular update of software patches for network equipment, antivirus etc. • Monitoring bandwidth utilization for the POP • Generating report and submit it to Project Manager (GSWAN). • Carry out feasibility surveys for new connectivity in the Taluka • Coordinate for VC events in Mamlatdar office and webcasting events in Taluka
18.	BMS/Facility Manager with Technical Background (24X7 Shift)	3	• PSO (Physical Security Officer) for operations of control room which includes CCTV, ACS, PRS, WLDS, FAS, FSS and other technical components required for smooth functioning of the Data Centre. • Good communication skills to be able to interact with vendors.
19.	Technical Assistant / Electrician	1	• Regular maintenance and daily check-up of DG Set, Transformer and HT Circuit Breaker, Power Cables, LT switch gear check-up and meter readings, Lighting Maintenance.

Note: It is clarified that the responsibilities and numbers mentioned against the position type are only indicative, it is the responsibility of bidder to provide requisite resources of right competency and experience to completely discharge functional requirements of Operations & management, Error reporting, SLA compliance, support (installation of applications, software, networking devices, OS, Storage, Backup) and the cost of such manpower should be part of the bid being quoted by the bidder.

2.33.2 The manpower deployed by the bidder for carrying out and providing services shall necessarily be Core resources except the following:

(a) Network Engineers (SCAN, DC & TC)

(b) Video Conferencing Engineers

(c) Electrical Assistant

2.33.3 Except the categories of O&M personnel listed above (2.33.2) all other remaining O&M resources deployed by the bidder should be on the bidders' payroll. The bidder may outsource the deployment of personnel listed above (2.33.2) to its existing partner engaged in the networking business at the time of bidding. The Network Engineers deployed must be B.E. with one year of relevant experience or Diploma Engineers with 2 years of relevant experience in handling network at Taluka Centres (TC) and BE with minimum 2 years of relevant experience at SCAN and District Centres (DC). The complete set of manpower resources proposed by the Bidder shall be on-site manpower only and strictly dedicated for this contract. Noncompliance of such deployment would result into imposition of penalty / termination of the contract as per the terms and conditions of RFP.

2.33.4 The manpower deployed by the bidder shall report to the respective nodal officers nominated by DST/GIL.

2.33.5 The Bidder has to provide supporting IT and Communication Infrastructure to such manpower, during entire contract period without any extra cost to the DST/GIL. Workspace shall be made available to the bidder by the concerned offices. Bidder has to ensure that the Support personnel deputed during all stages of the project shall carry an Identity Card duly authenticated by the DST/GIL.

Section III: Service Level Agreement (SLA)

3.1 SLA defines the terms of the O&M agency's responsibility in ensuring the performance of the network based on the agreed performance indicators as detailed in the agreement.

3.2 The table below summarizes the performance indicators for the services to be offered by the bidder. The detailed description of the performance indicators, SLA Terms and their definitions are elaborated in the following sections.

S.No	SLA Parameter	SLA Target
1	Network Availability between SC – DC	>=99.74 %
2	Network Availability between DC – TC , DC- other PoPs , TC- other PoPs	>=99.5%
3	Network Backbone Latency	Less than 50 ms
4	Network Backbone Packet Loss	<=1 %

3.3 Network SLA Terms & Definitions

S.No	SLA Terms	Description
1	Network Backbone	'Network Backbone' refers to Internet Protocol (IP) based routing infrastructure consisting network of selected GSWAN PoPs identified by the State at which, O&M Agency has installed network devices ("Selected PoPs") for Wide Area Network within the State.
2	Uptime	'Uptime' refers to GSWAN backbone availability across various segments i.e. between State Head Quarters to District Head Quarters and District Head Quarters to Taluka Head Quarters. "%Uptime" means ratio of 'up time' (in minutes) in a month to Total time (in minutes) in the month multiplied by 100.
3	Latency	'Latency' refers to the average time required for round-trip packet transfers between Selected PoPs on the selected portions of the

S.No	SLA Terms	Description
		GSWAN Backbone during a calendar month.
4	Packet Loss	'Packet Loss' refers to the average percentage of IP packets transmitted between Selected PoPs during a calendar month that are not successfully delivered.
5	Planned Network Outage	'Planned Network Outage' refers to unavailability of network services due to infrastructure maintenance activities such as configuration changes, up gradation or changes to any supporting infrastructure. Details related to such planned outage shall be approved by the DST/GIL or authorized authority and shall be notified to all the concerned stakeholder in advance (at least five working days). It is desirable that such outage shall be taken on Sundays or other Government holidays to the extent possible.
6	Unplanned Network Outage	'Unplanned Network Outage' refers to an instance in which no traffic can pass in or out through which users are connects to the GSWAN Backbone

3.4 GSWAN Backbone Latency

The Latency on the GSWAN Backbone shall be maintained at:

GSWAN Backbone Latency		
Network Segment	Network Latency	Remarks
SC – DC	50 ms	SLA allows a maximum of 50 Milliseconds in the connectivity between the State Head Quarter and to all the District Head Quarters.
DC – TC DC- other PoPs ,	50ms	SLA allows a maximum of 50 Milliseconds in the connectivity between the District Head Quarters to all the Taluka Headquarters.

TC- other PoPs		

3.5 GSWAN Backbone Packet Loss

The Packet Loss on the GSWAN Backbone shall be maintained typically at less than 1%.

SLA Parameter		**Packet Loss**
Network Segment	Packet Loss	Remarks
SC - DC , DC-TC DC- other PoPs , TC- other PoPs	<=1%	SLA allows a maximum of 1% of packet loss in the connectivity between the State Head Quarter and to all the District Head Quarters And between the District Head Quarters to all the Taluka Headquarters.

3.6 Denial of Service

3.6.1 Denial of Service (DoS) is the most common form of attack on the Network, which leads to network unavailability for the genuine network users. Successful Bidder shall respond to Denial of Service attacks reported by departments/ GSWAN users or GSWAN maintenance personnel within 15 minutes of intimation to the helpdesk. Denial of Service attack can be defined as sudden burst of network traffic leading to more than 90-95% utilization of the GSWAN bandwidth in any segment or complete network. In such a scenario operator shall perform an analysis of the issue, verify whether the network utilization is due to genuine user requirements or it is a denial of service attack. In case it is identified as DoS attack, operator shall identify the source of Denial of Service attack, and shall disconnect the source or network from GSWAN backbone and resolve the issue to ensure availability and performance of the backbone.

3.6.2 Successful bidder at regular intervals, shall monitor and measure the actual bandwidth allocated by the Bandwidth Provider against the agreed Committed Interface Rate (CIR) and issues identified shall be reported to DST/GIL and shall be escalated to the

Bandwidth Service provider for resolution.

3.7 Network Operations Management

3.7.1 Successful bidder is required to establish Contact Center (Helpdesk) at the State level with an appropriate Helpdesk tool. Helpdesk shall act as a SPOC (Single Point of Contact) for all the Network & Security related issues reported by the government departments or any other related stakeholders of the GSWAN. Each issue need to be recorded in the Helpdesk tool as a Service Request (with allocation of service request number) and the resolution timelines for such Service Requests shall be monitored by the State.

S.No	Severity	Initial Response Time	Issue Resolution Time
1	Level 1	15 Mins	1 Hr
2	Level 2	30 Mins	2 Hrs
3	Level 3	60 Mins	8 Hrs
4.	Level 4	240 Mins	24 Hrs

3.7.2 Severity Level Definition

Level 1:	The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services in State Head Quarter.
Level 2:	The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services in one or more Districts.
Level 3:	The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services to one or more departments in Sub division/ Taluka.

Level 4	The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services to one or more Horizontal Links

Section IV: Penalties

GSWAN

4.1 Successful Bidder shall be paid Quarterly Payment (QP) as per the services provided to DST/GIL. The overall penalty would be generally capped at 10% of QP amount. If the cap of overall penalty is reached in two consecutive quarters, the penalty cap for the third quarter onwards, for each quarter will increase by 5% over the penalty cap for the preceding quarter till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the DST/GIL shall be within its rights to undertake termination of contract if or anytime the penalty increases by 15 % of the QP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any quarter, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive quarters as referred above will reset and will begin afresh. Availability will be calculated on a quarterly basis.

Sl. No.	SLA	Target	Penalties in case of breach in SLA	Remarks
1	Network availability SC-DC Link	99.74%	a) 99.74% or Better= NIL b) 99.50% to 99.73%=0.25% of QP c) 99.00 to 99.49% = 0.50% of QP d) less than 99% = 0.75% of QP	.
2	Network availability DC – TC , DC- other PoPs , TC- other PoPs	99.50%	a) 99.50% or Better= NIL b) 99.00% to 99.49%=0.10% of QP c) 98.50 to 99.99% = 0.25% of QP d) less than 98.50% = 0.50% of QP	
3	Horizontal Links	Un escalated events/ incidents/faults to respective agencies for more than 4 hours from the time of detection	Rs. 100/- per hour per incident and part thereof	Bidders are responsible for O&M of horizontal links. This includes fault detection, analysis, and escalation to

				respective agencies within 4 hours of down-link reported in NMS or on help desk
4	GSWAN Backbone Latency	If the GSWAN Backbone Latency is more than the permissible limit as mentioned in SLA, Successful bidder has to analyze, report, escalate and get the issue resolved within 24 hours.	Rs. 2000 per hour, per instance or part thereof.	
5	**GSWAN Backbone Packet Loss**	If the GSWAN Backbone Packet Loss is more than the permissible limit as mentioned in SLA, Successful bidder has to analyze report, escalate and get the issue resolved within 6 hours.	Rs. 2000 per hour, per instance or part thereof.	
6	Delay or Non submission of Various MIS reports as mentioned in SLA	As mentioned in respective SLA	Rs. 1000 per instance per report	

Note: Above mentioned Penalties are all additive

4.2 Network availability

4.2.1 Network availability for a month is defined as total time (in minutes) in a month less total down time (in minutes) in a month excluding planned downtime. The network is considered available when all the services mentioned in the requirement section in full capacity are available. Bandwidth or Link downtime will not be considered as part of network downtime.

Network Uptime (%) =

Sum of total minutes during the Month - Sum of downtime minutes during the Month

---------- X 100

Sum of total minutes during the Month

4.2.2 Bidder will take at least 7 working days prior approval from the DST/GIL for the network maintenance i.e. planned downtime. Bidder's SLA and Penalty would be applicable only after final acceptance testing indicating that the link is completely functional. The Operator's request for payment shall be made at the end of each quarter by invoices along with the following supporting documents:

(a) Performance statistics

(b) Log of network parameters along with Service Down time calculation and Uptime percentage.

(c) Any other document necessary in support of the service performance acceptable to GoG.

4.2.3 The Quarterly Total Downtime will be the sum of the downtime incurred in each month. The deduction/penalty will be calculated on the Quarterly Total Downtime.

4.3 Penalty for not providing Video-conferencing/ Web casting services

If Successful Bidder fails to provide Video conferencing services or managing VC/Web casting mentioned in the scope of work, Rs. 1000 per incidence per location will be levied.

4.4 Penalty for non-keeping the control room up-to-date

If Successful Bidder fails to keep proper cooling, electrification, cabling, cleanliness, hygiene and safety requirements, various registers and network diagram as mentioned in the scope of work, Rs. 50000 per location per month will be levied.

4.5 Penalty for not providing technical feasibility and cost-estimation Report:

If Successful Bidder fails to provide technical feasibility report for expansion and laying of new horizontal links/POPS and effort and cost estimation of the same within 5 working days from the date of intimation from DST/GIL, as mentioned in scope of work, Rs. 1000 per feasibility per day or part thereof will be levied.

4.6 Penalties for delay in takeover

If successful bidder fails to complete the taking over of existing O&M of GSWAN and GSDC within the 45 working days from the project kick of date DST/GIL a Penalty of 0.50% of Quarterly Payment for each week of delay or part thereof shall be levied, until the completion of take over process and signoff from DST/GIL. If the delay continues beyond 12 weeks,

DST/GIL may terminate the Agreement and forfeit the PBG.

4.7 Penalty for Delay:

S. No.	Activity	Timeline	Penalty
1	Delay in Delivery/Supply of Hardware	T+ 60 days	0.5% of Contract value (as per Schedule-I of Price BID) per week or part thereof for delay in delivery (Delay beyond T+90days DST/GIL may terminate the contract and Forfeit the PBG).
2	Delay in Implementation	T+120 days	0.75% of Contract value (as per Schedule-I of Price BID) per week or part thereof for delay in delivery (Delay Beyond T+150 days DST/GIL may terminate the contract and Forfeit the PBG)
3	Delay in FAT	T + 180 days	0.10% of Contract value (as per Schedule-I of Price BID) per week or part thereof for delay in delivery

T= Kick off Date

Note: The above clause for penalties due to delay in FAT shall only be applicable for the delay attributed solely to the successful bidder as per his roles and responsibilities, delay due to other reasons shall not be considered.

4.8 Penalties for misuse

In case of misuse of bandwidth/ Internet at the instance of successful bidder, the penalty imposed on the successful bidder, without prejudice to other remedies available to DST/GIL under the Agreement, shall be 200% of annual value of bandwidth/Internet costs. If the misuse continues for two quarters, DST/GIL may terminate the Agreement

4.9 Penalties for not keeping man-power

If successful bidder does not deploy the required specified quantity & quality manpower as per

deployment plan of the proposed technical solution of the RFP or a person deployed is not reporting to the duty, there would be a penalty per person per day as defined below and will be deducted from the quarterly payment subject to a cap of 10% of the quarterly payment. If the above incidence occurs two times in one year, DST may reserve the right to terminate the contract and no payment would be done for the services rendered in that particular quarter.

Manpower penalties during the Operations stage		
Sl. No	**Penalty Clause**	**Penalty**
1	Successful bidder has to ensure that the number of personnel required as per Manpower clause 3.1 at the various operational levels of project The successful bidder shall ensure that alternate arrangements are made and leave for a staff is pre-sanctioned by DST/GIL If not, the penalties described in the following column shall apply (Any deviation in qualification or in experience of the deployed manpower will be treated as non-deployment for the purpose of penalty calculation)	1. Manpower at SC for O&M of GSWAN & GSDC: Rs. 10000/- per day per person for un-sanctioned/ non-reporting. 2. Manpower at DC: Rs. 2000 per person per day of unsanctioned leave or non-reporting or non-deployment. 3. Manpower at TC & PoP Rs. 1000 per person per day of unsanctioned leave or non-reporting or non-deployment.

Note: Bidder has to provide attendance Report of all manpower deployed every month, penalty of INR 10000/- per month shall be levied for delay in submission of attendance report.

4.10 **Penalty for Delay in taking Insurance**: Successful bidder will take insurance of the equipment under O&M within Six months from the date of signing of contract. Penalty of INR 1 lakh per month after six months from the kick of date shall be levied.

4.11 **Penalty for delay in replacement of batteries:** If Successful Bidder fails to replace the internal as well as external battery banks used for UPS and other equipments at SC,DC,TC & other PoPs with new batteries two times during the contract period of 5 years as mentioned in scope of work i.e. during 9th quarter and 17th quarter of the O&M services, to begin with 5% QP of the 9th and 17th quarter would be withheld. In case the replacement of batteries is delayed beyond 10th and 18th quarter, the withheld amount shall be forfeited and from subsequent payment due, penalty @5% of the quarterly payment due will be levied till the replacement is made. Moreover, such non-performance of the scope of work may result into termination of contract. This penalty shall be exclusive of all other penalties proposed under the contract.

4.12 SLAs for GSDC

Sl. No.	SLA	Target	Penalties in case of breach in SLA	Remarks
1	Uptime of all IT components & services under scope	99.741% (at each individual component level)	For each 0.5 slab (lower) a penalty 1.0 % on QP shall be charged for each component.	For each component 99.241-99.741 - 1.0% of QP 98.741-99.241 - 2.0% of QP And so on If the uptime goes below 96.741, additional penalty of 1% will be charged on QP for each slab 1% downtime.
2	Uptime of all non-IT Components & services under scope	99.741% (at each individual component level)	For each 0.5 slab (lower) a penalty 0.50% on QP shall be charged for each component	99.249-99.749 - 0.5% of QP 98.749-99.249 - 1.0% of QP And so on If the uptime goes below 96.749%, additional penalty of 0.5% will be charged on QP for a slab of 1%.
3	Closure of Audit Findings	100.000%	• Rs.10000/- per day delay for closure of each high and medium classified audit finding • Rs. 2000/- per day delay for closure of each low classified audit finding	Periodic Audits will be conducted by DST or DST Authorized personnel, the Audit Findings shall be closed by the O&M Agency As per the closure schedule defined by the Auditor. If there is any delay in closing the audit findings then penalties will be levied.
4	Incident Resolution	Priority Level 1 Incident - Within 1 hr Priority Level 2 Incident - Within 12 hr Priority Level 3 Incident -	level 1 Incident 0.25% of QP for every 2 hr delay in resolution; Level 2 Incident 0.25% of QP for every 6 Hr delay in resolution; Level 3 Incident 0.25% of QP for every 12 hrs delay in resolution	Incidents will be logged in the Helpdesk and the O&M Agency will have to resolve the incident and provide necessary updates through the Help Desk Portal and co-ordinate

		Within 24 hr		with the stakeholders. Root Cause should be identified for all incidents; if root cause is not identified then additional penalties will be levied.
5	Request Resolution	Priority Level 1 Incident - Within 2 hr Priority Level 2 Incident - Within 24 hr Priority Level 3 Incident - Within 36 hr	level 1 Incident 0.25% of QP for every 2 hr delay in resolution; Level 2 Incident 0.25% of QP for every 12 Hr delay in resolution; Level 3 Incident 0.25% of QP for every 18 hrs delay in resolution	Requests (like e-mail password reset, firewall port opening, hardening...etc) will be logged in the Helpdesk and the O&M Agency will have to resolve the request and provide necessary updates through the Help Desk Portal and co-ordinate with the stakeholders.
6	Security Breach	Detection of security Breach - within 30 minutes Mitigation of Security Breach - within 1 hr from the time of Breach	3% Of QP for every 30 minutes delay in detection and additional 1% for every 1 hr delay in the mitigation of security breach	The security breach will include but not limited to successful penetration of any Virus, trojan, malwares, zero-day attacks, intrusion, Denial of Service Attacks, …etc, up to the server level. In case of any compromise of data due to the Security Breach then double penalty will be levied (this will not be counted within the maximum penalty cap limit).

Note: Above mentioned Penalties are all additive