GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS
DIGITAL BHARAT NIDHI

REQUEST FOR PROPOSAL (RFP)
For
Selection of Managed Service Provider for Migration, Hosting & Operations of IT applications of Digital Bharat Nidhi on MeitY empanelled Cloud

RFP No.: 30-40/2022/USOF/PMU/Part-II;
Date: 27.12.2024

Schedule of Events:

S. No.	Key Activities	Date
1	Issuance of Request for Proposal (RFP)	30.12.2024
2	Last date of receiving queries from bidders	03.01.2025
3	Pre-bid meeting date	06.01.2025 at 11:00 AM at 3rd Floor, Block A, East Kidwai Nagar, New Delhi, 110023
4	Last date and time for submission of e-bids	20.01.2025 by 01:00 PM
5	Opening of the e-bid -Technical Proposal	20.01.2025 at 01:30 AM
6	Technical Presentation	To be intimated
7	Opening of the e-bid - Financial Proposal	To be intimated
8	Contract Finalization and Award	To be intimated

Contents

Disclaimer:

1. This RFP is not an offer by Digital Bharat Nidhi (DBN), Department of Telecommunications, Ministry of Communications, Government of India, but an invitation to receive electronic proposals from interested and eligible bidders for Selection of Managed Service Provider for Migration, Hosting & Operations of IT applications of Digital Bharat Nidhi (DBN) on MeitY empanelled Cloud.
2. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed between DBN and the successful bidder.
3. This RFP is being issued with no financial commitment and the DBN reserves the right to withdraw the RFP and change or amend any part thereof or foreclose the same at any stage.
4. The information contained in this Request for Proposal (RFP) Document is being provided to interested bidders on the terms and conditions specified in this RFP document. The purpose of this RFP Document is to provide interested parties with information that may be useful to them in submitting their proposal in response to this RFP.
5. Although every effort to provide the accurate details have been made in this RFP document, however, while preparation of the proposal, if any or some of the conditions are ambiguous and are not explicitly clear, the same may be clarified before submission of proposal. DBN shall not be responsible for any kind of mis-conceived interpretation at bidder's end.
6. Information provided in this RFP are solely for the purpose of engaging a Managed Service Provider for migration and hosting of existing applications of DBN to MeitY empanelled cloud and thereafter consequent management of the same. Use of the information provided in this document for any other reference will be the sole responsibility of the bidder and DBN shall not be liable in any way, whatsoever.
7. This RFP, an integral part of the RFP Document, serves the limited purpose of invitation for Selection of Managed Service Provider for Migration, Hosting & Operations of IT applications of Digital Bharat Nidhi on MeitY empanelled Cloud. 'This RFP gives a salient summary of the relevant information, including the Type of BPQ/ Contract and Selection Method to evaluate RFP. However, Bidders must go through the complete RFP Document for details before submission of their Proposals.
8. The RFP Document does not purport to contain all the information. Bidder(s) may require. It may not address the needs of all Bidders. They should conduct due diligence, investigation, and analysis, check the information's accuracy, reliability, and completeness, and obtain independent advice from appropriate sources. Information provided in the RFP Document to the Bidder(s) is on various matters, some of which may depend upon interpreting the law. The information given is not an exhaustive account of statutory requirements and should not be regarded as complete or authoritative statement of law. DBN, its employees and other associated agencies accept no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.
9. DBN, its employees and other associated agencies make no representation or warranty for the accuracy, adequacy, correctness, completeness or reliability of any assessment, assumption, statement, or information in the RFP Document. They have no legal liability, whether resulting

from negligence or otherwise, for any loss, damages, cost, or expense arising from/ incurred/ suffered, howsoever caused, to any person, including any Bidder, on such account. DBN may, at its absolute discretion amend or supplement the information, assessment or assumptions contained in this RFP document. DBN reserves the right to reject any or all of the bids without assigning any reason whatsoever.

10. Bidders shall bear all costs pertaining to preparation and submission of its Bid including but not limited to preparation, copying, postage, e-signing, expenses etc. All such costs and expenses will remain with the Bidder and DBN shall not be liable in any manner whatsoever for such or any other costs or other expenses incurred by a Bidder while preparation or submission of the Bid, irrespective of the outcome of the Bidding Process.

Abbreviations:

Sr. No.	Abbreviation	Explanation
1.	BG	Bank Guarantee
2.	BoM	Bill of Material
3.	CERT-In	Indian Computer Emergency Response Team
4.	CMMI	Capability Maturity Model Integration
5.	CSP	Cloud Service Provider
6.	DB	Database
7.	DBN	Digital Bharat Nidhi (Erstwhile Universal Services Obligations Fund)
8.	DD	Demand Draft
9.	DDoS	Distributed Denial of Services
10.	DMZ	Demilitarized Zone
11.	DoT	Department of Telecommunications, Ministry of Communications, GoI
12.	DR	Disaster Recovery
13.	EMD	Earnest Money Deposit
14.	EMS	Enterprise Management System
15.	GDPR	Global Data Protection Regulation
16.	GeM	Government e-Marketplace
17.	GIGW	Guidelines for Indian Government Websites
18.	GoI	Government of India
19.	GST	Goods and Services Tax
20.	GUI	Graphical User Interface
21.	HSM	Hardware Security Module
22.	IaaS	Infra as a Service
23.	IAM	Identity and Access Management
24.	ICT	Information and Communication Technology
25.	IMEI	International Mobile Equipment Identity
26.	INR	Indian National Rupee
27.	IPR	Intellectual Property Rights
28.	IPS	Intrusion Prevention System
29.	IPV	Internet Protocol Version
30.	ISO	International Organization for Standardization
31.	ISP	Internet Service Provider

Sr. No.	Abbreviation	Explanation
32.	IT	Information Technology
33.	ITeS	Information Technology enabled Services
34.	ITIL	Information Technology Infrastructure Library
35.	ITSM	Information Technology Service Management
36.	LoA	Letter of Acceptance
37.	MeitY	Ministry of Electronics and Information Technology, Government of India
38.	MFA	Multi Factor Authentication
39.	MIS	Management Information System
40.	MSP	Managed Service Provider also called as “Bidder”
41.	NIC	National Informatics Center
42.	O & M	Operations and Maintenance
43.	OWASP	Open Web Application Security Project
44.	PaaS	Platform as a Service
45.	PBG	Performance Bank Guarantee
46.	PO	Purchase Orders
47.	QCBS	Quality cum Cost Based Selection
48.	RDBMS	Relational Database Management System
49.	REST	Representational State Transfer
50.	RFP	Request for Proposal
51.	SIEM	Security Information and Event Management
52.	SLA	Service Level Agreement
53.	SoA	Service-oriented Architecture
54.	SSL	Secure Socket Layer
55.	TTDF	Telecom Technology Development Fund
56.	UAT	User Acceptance Testing
57.	USOF	Universal Service Obligation Fund
58.	VPN	Virtual Private Network
59.	WAF	Windows Application Firewall

1. Introduction:

1.1 About Digital Bharat Nidhi (DBN) (Erstwhile Universal Service Obligation Fund or USOF): DBN primarily engages itself to adequately serve backward and rural areas to enhance telecom connectivity. Keeping in mind the inadequacy of the market mechanism to serve rural and inaccessible areas on one hand and the importance of providing vital telecom connectivity on the other, the New Telecom Policy, 1999 provisioned for resources for meeting the Universal Service Obligation (USO) to be raised through a 'Universal Access Levy (UAL)', being a percentage of the revenue earned by the operators under various licenses. The Universal Service Support Policy came into effect from 01.04.2002. The Indian Telegraph (Amendment) Act, 2003 giving statutory status to the Universal Service Obligation Fund (USOF) was passed by both Houses of Parliament in December 2003. The Rules for administration of the Fund known as Indian Telegraph (Amendment) Rules, 2004 were notified on 26.03.2004. As per the Indian Telegraph Act 1885 (as amended in 2003, 2006 and 2008), the Fund is to be utilized exclusively for meeting the Universal Service Obligation.

1.2 DBN aims to drive digital transformation and modernization of government operations by leveraging cloud technologies and has been established to formulate and execute various projects keeping in mind the above goals and objectives. Following are the functions of DBN:

i. Formulating and executing DBN projects or schemes.
ii. Monitoring the implementation of DBN projects and schemes.
iii. Accurate and timely financial support for all DBN projects.
iv. Ensuring adherence to DBN guidelines.
v. Designing subsidy support model for reducing the viability gap.
vi. Determining desirable subsidy level, structure and disbursement schedule.
vii. Post-implementation review of USOF projects and schemes.
viii. Leveraging of innovative and emerging new technologies.
ix. Standardising practices and documentation of DBN projects.
x. Strategic partnerships with Industry and Universal Service Providers (USPs).
xi. Collaborating with international organizations.
xii. Benchmarking of international best practices.

1.3 About the RFP Requirement: The applications developed by DBN are being utilized to derive the data of mobile towers from various telecom circles and the derived data are being monitored and evaluated for taking further decisions.

DBN, through this RFP, intends to appoint a Managed Service Provider (MSP) for migration and operations of existing Digital assets of DBN to cloud from existing servers through Cloud Service Providers (hereinafter CSP). CSP shall be a MeitY empanelled Cloud Service Provider (CSP) who can deliver scalable, secure, and cost-effective cloud services for a period of 24 months extendable for another 12 months on same terms and conditions. The requirement is to enhance DBN s existing and upcoming IT infrastructure by adopting cloud technology that will ensure high availability, scalability, security, flexibility, support etc for execution of various government programs and services.

1.4 Existing Applications Details:

a. Website of DBN
b. Project Management Information System
c. Telecom Technology Development Fund
d. Dashboard, MIS and Reports
e. New CSMS 2.0, updated version of PMIS & Dashboards, BharatNet & BNU

2. Scope of Work:

The Scope of Work for this RFP encompasses a comprehensive range of tasks and responsibilities to be executed by the selected Service Provider for the DBN initiatives.

Following are the broad categories of work to be executed by the selected bidder, however bidder maybe required to perform such additional tasks that may be required to perform the operations smoothly:

a. **Assessment of existing Systems:** Selected bidder / MSP shall be required to perform a thorough As-Is assessment of the existing infra and usability of the applications so that the same can be migrated to MeitY empanelled Cloud. Assessment includes the technical as well as operational functions of the applications and infrastructure associated therewith.
At present, the Applications are hosted on NIC Cloud environment and being managed by inhouse team of DBN.

b. **Cloud Infrastructure Provisioning:** The bidder shall be required to provision, implement, and maintain a robust cloud infrastructure. This infrastructure must adhere to high availability standards, ensuring minimal downtime and maximum performance.
The architecture must support the seamless integration of various cloud services, enabling efficient resource management and scalability to accommodate fluctuating demands.

c. **Migration of Existing Systems:** The bidder will be responsible for developing a detailed migration strategy for transitioning of existing IT systems and applications to the cloud environment. This strategy should encompass planning, execution, and validation phases to ensure successful migration.
During the migration process, bidder must ensure no disruption to ongoing operations, including the formulation of a rollback plan to revert to existing systems if required.

d. **Management of Cloud Services:** The bidder shall provide ongoing management and monitoring of cloud resources to ensure optimal performance, reliability, and security. This includes the use of automated tools to facilitate resource allocation, scaling, and load balancing.
The bidder shall be required to implement a comprehensive monitoring system that provides real-time insights into resource utilization, performance metrics, and potential security threats.

e. **Support, Maintenance and SLA:** The bidder should offer responsive and knowledgeable technical support to address any issues or queries promptly. The bidder is required to offer 24/7 technical support to address any issues related to cloud operations. This support shall

include a ticketing system for problem resolution, regular maintenance schedules, and proactive system health checks. All maintenance activities must be performed in accordance with defined Service Level Agreements (SLAs) to ensure availability and performance standards as per prescribed SLAs. The selected bidder shall ensure that a dedicated team of support staff are always available for problem resolution and other issues incidental thereto, for DBN.

f. **Compliance and Security Management:** The bidder shall ensure that all cloud services comply with applicable government regulations, data privacy laws, and security protocols throughout the deployment and operational phases.
Implementation of stringent security measures, including data encryption, access controls, regular security audits, and vulnerability assessments, is mandatory to safeguard sensitive government data.

g. **Monitoring, Reporting and Documentation:** The bidder shall provide regular monthly reports detailing service performance, usage metrics, compliance with SLAs and any and all incidents of outages encountered.
Comprehensive documentation related to system configurations, operational processes, and compliance audits must be maintained and made available to DBN upon request.

Following are the broad requirements from the CSP:

a. **Scalability and Elasticity:** The cloud hosting solution should provide the ability to easily scale resources up or down based on demand, allowing seamless expansion or contraction of infrastructure as needed. Elasticity should enable automatic allocation and deallocation of resources to accommodate varying workloads without manual intervention.
b. **High Availability and Fault Tolerance:** The cloud hosting platform must ensure a high level of availability by distributing resources across multiple data centres or regions to mitigate the impact of potential failures. It should have built-in redundancy and fault tolerance mechanisms to maintain service continuity.
c. **Security and Data Protection:** The bidder should implement robust security measures to protect data against unauthorized access, breaches and loss. Encryption of data at rest and in transit should be supported with adherence to industry-standard security protocols and certifications. Bidder should automatically encrypt data both in transit outside of physical boundaries not controlled by CSP and at rest by default and provide multiple ways to control encryption keys and data access
d. **Performance and Reliability:** The cloud hosting solution must offer reliable and consistent performance, with low latency and high throughput to meet application requirements. Service-level agreements (SLAs) are in place to ensure a certain level of performance, uptime and response time.
e. **Compliance and Governance:** The CSP should comply with relevant industry regulations and standards, such as GDPR as applicable in this project, ISO 27001, CMMI etc to ensure the protection of sensitive data. Clear documentation and audit trails should be available to demonstrate compliance with applicable governance requirements.
f. **Integration and Interoperability:** The cloud hosting platform should support easy integration with existing systems, applications and APIs to enable seamless data flow and

interoperability. Compatibility with popular programming languages, frameworks and tools should be ensured to facilitate development and deployment processes.

g. **Monitoring and Analytics:** Comprehensive monitoring and analytical capabilities should be available to track and analyse the performance, utilization and health of the cloud hosting infrastructure and applications. Real-time alerts and reporting mechanisms should enable proactive identification and resolution of potential issues.
   Note: Management of existing applications is NOT in the scope of proposed MSP, IT team/s of the DBN is managing the application.

h. **Management of Existing Applications:** It is explicitly made clear that MSP's scope of work won't include the management of existing applications of DBN. However, the MSP shall always coordinate with the existing application team of DBN for any doubt or such other clarifications, as may be required, in the course of migration and hosting of existing applications of DBN over the cloud.

3. Technical Requirements:

3.1. Hosting on a MeitY empanelled Cloud:

The selected bidder shall be required to undertake below mentioned services, during the subsistence of Agreement, to provide adequate allocation of resources on cloud on actuals basis, ensure availability of applications as per the defined SLAs. Mentioned below are the detailed descriptions of services, including but not limited to, that the bidder shall be responsible to provide during the subsistence of the Agreement. Bidder shall also be required to assess and include any other services, apart from mentioned below, that may be provisioned to provide end to end solution, either provisioned by DBN or by the Bidder at its own so as to ensure smooth migration, hosting and subsequent management of applications of DBN:

i. Provisioning of required and necessary IT infrastructure (server, databases, storage space, security services, network connectivity, containers etc.) at all the time through a self-service/orchestration platform.
ii. The bidder shall be responsible for management and allocation of necessary IT infrastructure (compute, storage, security, network etc.) on cloud enabling all the applications to perform at the optimum level and in line with the SLAs defined.
iii. Public facing services can be deployed in a demilitarized zone (DMZ) different from the application services. The Database node should be in a separate zone with higher security layer.
iv. Bidder shall create different environments in cloud as per the requirement of the project. The non-production environments (if required) shall be separated from the production environment.
v. VMs Instances should support both 1:1 and 1:2 ratio of physical to virtual core only; but should not be more than 1:2.
vi. Physical CPU in the cloud platform should be of the latest generation, not released before 2021
vii. Bidder shall provide all required support with regards to available APIs, data portability, migration etc., to the DBN to utilize in case of change of cloud service provider, migration back to NIC cloud or to a different cloud service provider.
viii. Should adhere to the relevant standards published (or to be published) by but not limited to MeitY, STQC, CERT-IN, I4C etc.

ix. The empanelled cloud service offerings must comply with the additional guidelines/standards (applicable for the Empanelled Cloud Service Offerings) as and when such guidelines/standards are published by MeitY at no additional cost to retain the empanelment status.
x. Bidder shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.
xi. The empanelled cloud service offerings must comply with the additional guidelines / standards (applicable for the Empanelled Cloud Service Offerings) as and when such guidelines / standards are published by MeitY at no additional cost to retain the empanelment status.
xii. Bidder should provide a code-free graphical interface that delivers point-and-click data integration that supports custom connections and transformations with a Low-code/No-Code approach
xiii. Bidder should have capability of both IaaS and PaaS in their cloud setup so that DBN take leverage of such offerings as and when required time to time.
xiv. Solution shall enable ease of infrastructure management, shall be agnostic to the underlying hardware, storage, network, operating system and hypervisor and shall support open format for virtual machine images. The cloud architecture shall be scalable to meet future demand and provide requisite levels of security and interoperability to host DBN's critical infrastructure on cloud in safe environment.
xv. The cloud hosting solution should provide features such as flexible pricing models, flexible utilization of the resources as well as separate billing on the basis of consumption by the DBN
xvi. Bidder shall be responsible for hosting the existing applications on cloud platform on Platform as a Service (PaaS)/Infra as a Service (IaaS) model. The hosting of the application should be carried out in at least Tier III Data Centre within India. Bidder shall be required to submit MeitY empanelment certificate issued to the Cloud Service Provider along with the technical proposal.
xvii. The Bidder shall have proper DR backup and restoration mechanism, in addition to escalation procedure and emergency response in case of failure/disaster at DC.
xviii. Bidder will be responsible for installation of all the software required for the successful hosting of the applications in the Data Centre.
xix. Cloud platform should provide sufficient capacity for data processing, data storage and network bandwidth to handle the overall load and traffic coming to the applications without compromising the overall performance of the system. The cloud service should provide dedicated IP, dedicated SSL/TLS certificate.
xx. It will be the responsibility of bidder to prepare the specification for cloud platform i.e., CPUs, RAM, storage, required software, other equipment and the network requirements for running the applications efficiently.
xxi. The bidder shall formulate an effective Back-up Strategy and Disaster Recovery Plan and shall be responsible for implementing the same at the time of migration and commissioning of Digital Bharat Nidhi Applications in case if required in future.
xxii. The bidder shall also ensure that the hosting services should be portable to another vendor without any changes to hosting environment in case of requirement.
xxiii. It is mandated that bidder shall host the applications on the MeitY empanelled CSPs only. In no case, bidder shall host the application on cloud platform of any company which has a history of data loss and security breaches.
xxiv. The Cloud Infrastructure shall be capable of catering growth and integration requirements etc. for entire contract period.

xxv. Bidder shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions are working on timely basis and a schedule against the same shall be communicated in advanced to the DBN.

xxvi. Monitor VMs up/down status and resource utilization such as RAM, CPU, Disk, input/output operations per second (IOPS) and network through the use of CSP native orchestration tool/dashboard, the reports for the same shall be submitted as part of documentary evidence during monthly billing.

xxvii. Provide hardware or software based virtual load balancer services (VLBS) through a secure, hardened, redundant Managed Virtual Load Balancer platform.

xxviii. Provide anti-virus protection and OS level security as per standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation.

xxix. DBN retains the right to request full copies of the virtual machines at any time.

xxx. DBN retains full ownership of all loaded software installed on virtual machines and any application or product that is deployed on the Cloud by selected bidder. The Bidder shall take utmost care in maintaining security, confidentiality and backup of this data

xxxi. Bidder shall adequately size the necessary compute, storage and other cloud services required, building the redundancy wherever necessary into the architecture and load balancing to meet the service levels.

xxxii. While the initial sizing and provisioning of the underlying infrastructure may be carried out based on the information provided in the RFP document, subsequently, it is expected that the bidder, based on the growth in the user load (peak and non-peak periods; year-on-year increase), shall scale up or scale down the compute, memory, and storage as per the performance requirements needed to run all modules of DBN applications in a seamless manner and meet the SLAs using the auto-scaling features (through an user-friendly dashboard).

xxxiii. In addition to auto-scaling, for any major expected increase in the workloads, carry out the capacity planning in advance to identify and provision, where necessary, the additional capacity to meet the user growth and/or the peak load requirements to support the scalability and performance requirements.

xxxiv. The scaling up/scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits must be changed) must be carried out with prior approval by DBN. The bidder shall provide the necessary details including the sizing calculations, assumptions, current workloads and utilizations, expected growth/demand and any other details justifying the request to scale up or scale down. These requests shall be made prior to actual usage considering the future demand based on usages.

xxxv. Setup, configure and manage Virtual machines, containers. Storage (block, object etc., as applicable). Network and security (public subnets, private subnets, security rules, VLAN etc.). Identity and access management, database and database administration tasks. Managed Load Balancer. Managed Firewall, Built-in security like IDS/IPS, DDoS mitigation, SSL Interceptor firewall etc. shall be provided in the cloud platform.

xxxvi. Backups, snapshots of application servers, applications, databases and its archival, retrieval, access, authorization monitoring of all instances and reporting of failure as per SLA. Provide access to monitor health/system utilization through a dashboard. Monitoring all cloud services used for an application and fixing of issues, if any.

xxxvii. Generate email alerts for all major problems in the cloud infrastructure and application. Managed services include Database Management, its backup and restoration and Operating System Management.

xxxviii. Cloud service shall support auditing with features such as “what request was made”, “the source IP address from which the request was made”, “who made the request”, “when it was made” etc.

xxxix. Shall facilitate the use of different types of disks like SAS, SSD etc. based on type of application.

xl. Bidder shall ensure the availability of services online 24X7 basis, on-demand and dynamically scalable up or down as per request for service with two factor authentications through a secure web browser and provide scalable, redundant, dynamic storage.

xli. Bidder shall provide a redundant local area network (LAN) infrastructure and static IP addresses or “private” non-internet routable addresses.

xlii. Bidder shall be able to deploy VMs in multiple security zones, as required for the project, defined by network isolation layer.

xliii. Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP). Provide IP address and IP port assignment on external network interfaces.

xliv. Bidder shall configure the DBN provided domain name on its servers and provide dedicated virtual private network (VPN) connectivity.

xlv. Allow mapping of IP addresses to domains owned by the DBN, allowing websites or other applications operating in the cloud to be viewed externally as Government URLs and services.

xlvi. Bidder shall support for providing secure connection to DC Site to DBN department or any hired third-party auditing agency.

xlvii. DC Site shall support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs for various types of user entities. Provision must be made for segregation of access path among various user categories.

xlviii. Solution shall support network level redundancy for network connectivity with at least two different service providers. These two networks shall not share same back-end infrastructure. Redundancy in security and load balancers, in high availability mode, shall be provided to facilitate alternate paths in the network.

xlix. The CSP should provide native dashboard for SLA Monitoring and Reporting of Service Uptime

The CSP should provide API to manage Cloud Infrastructure for deployment and management of cloud infrastructure

3.2. Virtual Machine Requirements:

i. Bidder shall ensure availability of online services, on-demand and dynamically scalable (up or down) as per the request for service with two factor authentications through a secure web browser via public internet

ii. The services provided shall be auto-scalable, redundant and shall have dynamic computing capabilities of virtual machines

iii. Solution shall perform an image backup of Virtual Machine (VM) image information or support the ability to take an existing running instance or a copy of an instance and export the instance into approved image format

iv. In case of suspension of a running VM, the VM shall still be available for reactivation for reasonable time without having to reinstall or reconfigure the VM. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed

and shall confirm DBN for VM and data destruction and shall ensure that the data cannot be forensically recovered.

v. Bidder shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions are working on timely basis and a schedule against the same shall be communicated in advance.

vi. Monitor VMs up/down status and resource utilization such as RAM, CPU, Disk, input/output operations per second (IOPS) and network through the use of orchestration tool/dashboard, the reports for the same shall be submitted as part of documentary evidence during monthly billing

3.3. Central Processing Unit (CPU) Requirements:

i. A minimum equivalent CPU processor speed of 3.0 GHz shall be provided.
ii. The CPU shall support 64-bit operations
iii. Provide hardware or software based virtual load balancer services (VLBS) through a secure, hardened, redundant Managed Virtual Load Balancer platform.
iv. Provide hardware or software based virtual load balancing as a service to deliver stateful failover and enable O&M manpower to distribute traffic load across multiple servers.

3.4. Operating System (OS):

i. Service shall support one or more of the major OS such as Windows, LINUX, Ubuntu and other currently supported OS
ii. Management of the OS processes and log files including security logs retained in guest VMs

3.5. Security Requirements:

i. Provide anti-virus protection

ii. Provide OS level security as per standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation

3.6. Storage Requirement:

i. Shall facilitate the use of different types of disks like SAS, SSD based on type of application.
ii. Bidder shall ensure the availability of services online 24X7 basis, on-demand, and dynamically scalable up or down as per request for service with two factor authentications through a secure web browser and provide scalable, redundant, dynamic storage.

iii. There shall not be any additional cost associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for any data of/related to DBN.

iv. Service shall provide scalable, redundant, dynamic storage

3.7. Network and IP Requirements:

i. Bidder shall provide a redundant local area network (LAN) infrastructure and static IP addresses or “private” non-internet routable addresses.

ii. Bidder shall be able to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers.

3.8. IP Addressing:

i. Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).

ii. Provide IP address and IP port assignment on external network interfaces.

iii. Provide dedicated virtual private network (VPN) connectivity.

iv. Allow mapping of IP addresses to domains owned by the DBN, allowing websites or other applications operating in the cloud to be viewed externally as Government URLs and services.

v. Bidder shall ensure the cloud infrastructure provided is IPv6 compliant.

vi. Bidder shall support for providing secure connection to DC Site to DBN or any hired third-party auditing agency.

vii. Solution shall support network level redundancy for Internet lines with two different service providers. These two networks shall not share same back-end infrastructure. Redundancy in security and load balancers, in high availability mode, shall be provided to facilitate alternate paths in the network.

3.9. Network Security:

i. All possible environments (Dev/Quality/Pre-Prod/Prod) and zones (DMZ, MZ, shared, and private) should be segmented from one another either logically or physically.

ii. System shall have capability to protect network subnets with access controls that provides an optional layer of security that provides a stateless firewall for controlling traffic in and out of a subnet.

iii. System shall have capability to segregate public subnet and private subnet.

iv. System shall have capability to configure route tables that define which subnets are allowed to route external traffic over backend VPN or site-site connections, peering connections, Internet connections, or even specific virtual machine instances.

v. System shall prevent packet sniffing: Virtual instances should be designed to prevent other instances running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance. Even if tenants configure interfaces into promiscuous mode, the hypervisor should not deliver any traffic to them that is not addressed to them.

vi. System shall prevent IP Spoofing: The Cloud service should not permit an instance to send traffic with a source IP or MAC address other than its own.

vii. All inbound and outbound traffic between Internet and different segments shall be routed through Firewall solution.

viii. Firewall solution shall perform stateful inspection of traffic from layer-3 to layer-7.

ix. Firewall solution shall provide complete control and visibility to Layer 3-7 network traffic for all the segments.

x. Firewall solution shall be capable of decrypting and then encrypting SSL traffic.

xi. Firewall solution shall have capability of threat prevention against threats like exploits, vulnerabilities, Intrusion (IPS), virus, spywares, known malwares etc.

xii. Solution shall allow creation of policy/rule based on source IP/port, destination IP/port, application, domain, protocol, and geo-location.

xiii. Firewall solution shall support integration with DevOps tools, Configuration management tools and Provisioning tools like Terraform, Chef, Ansible etc for deployment, if required.

xiv. Firewall solution should integrate with Native cloud services for automatic scaling to increase performance and availability.

xv. Firewall solution shall offer web filtering that can stop traffic to known-bad URLs and monitor fully qualified domain names.

3.10. Data Governance and Security:

i. Solution shall be based on Zero Trust Model security architecture which means that by default, not everyone is trusted from inside or outside the network, and verification is mandatory for everyone trying to access the resources on the network. This additional layer of security has been introduced to prevent data breaches.

ii. Micro-segmentation for workloads thereby having a capability to monitor and restrict East-West communication based on the need.

iii. Solution shall have macro and micro level segmentations to provide defence-in-depth secured architecture.

iv. The Data Governance and Security Framework being put by the bidder should ensure that the granularity of the data access should be maintained.

v. Configuration and management access shall be available to admin users using IAM.

vi. Scaling of the Security Resources of the project shall be automatic. Security component shall be able to scale as per the application/API usage. Resources of the security products like CPU, Memory, Throughput, Latency etc shall not be a bottleneck for the whole project during the runtime.

vii. Data shall not leave the boundaries of the country and data residing within Cloud shall not be accessed by any entity outside the control of Dept. /authorized representative of DBN.

viii. The solution should be able to discover all provisioned resources and provide details such as configuration items inventory, history of changes to such configuration items, snapshot

of resource inventory at a single point in past, set-up of policies to track provision of resources within a client defined rulesets and auto-notifications (based on notification severity level) each time, whenever a configuration change happens and it should be configurable by administrator.

ix. Security shall be built in automated software build pipelines with continuous integration and continuous delivery (CI/CD) and agile development methodologies.

x. It is recommended that the bidder should follow the eSAFE (e-Governance Security Assurance Framework) Guidelines for Implementation of Security Controls issued by the Ministry of Electronics and Information Technology (MeitY), Government of India.

xi. CERT-In guidelines, GOI (Govt of India) guidelines on application security shall be followed.

xii. Unauthorized access should be restricted and only authorized users with valid authentication shall be allowed to access.

xiii. The Solution should have the capability to log every possible detail of user actions, data access and changes. The system should store last 6 months of such log beyond which the same would be archived in retrievable format. The logs present in the system should conform to the Indian IT Act and should uphold legal sanctity under Indian Laws.

xiv. The bidder shall be responsible for ensuring security of the solution from any threats and vulnerabilities. The bidder shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/detection, content filtering and blocking, virus protection, event logging & correlation and vulnerability protection through implementation of proper patches and rules.

xv. The bidder shall ensure proper end point protection for any VM based Solution.

xvi. The Solution should have audit and compliance features which enables DBN to monitor the provisioned resources, performance, resource utilization, and security compliance.

xvii. The solution shall have capabilities to continuously monitor for malicious or unauthorized behaviour. Bidder shall deploy manpower for continuous monitoring of logs, attacks, malicious or unauthorized behaviour.

xviii. Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

xix. Solution shall apply security measures like ‘captcha’ at the time of login by user in web portals/Mobile apps to determine whether the user is human or not, and to avoid unauthorized access by Other Software i.e., Bots etc.

3.11. Database Activity Monitoring:

I. The database activity monitoring solution should encompass a comprehensive set of capabilities, such as discovery and classification, vulnerability management, application-

level analysis, intrusion prevention, support for unstructured data security, identity and access management integration, and risk management support.

II. The solution should monitor multiple database servers and multiple versions of each server according to the database proposed by bidder. All network-based database activities should be monitored.

III. The solution should keep all the audit trail tamperproof and be managed centrally.

IV. The solution should have the ability to aggregate, normalize and correlate activity from multiple heterogeneous Data Base Management Systems (DBMS)

V. The solution should provide automated discovery of both new and existing Database tables.

VI. The solution support identification of rogue or test databases.

VII. The solution should detect sensitive data types, including but not limited to credit card numbers in database objects

VIII. The solution should ensure that default database accounts do not have a “default” password.

IX. The solution should have pre-defined reports covering compliance, non-technical, incident, and general technical reports.

X. The product should support custom report generation with an option to distribute reports on demand and automatically (on schedule).

XI. The solution should capture Select, update, insert, and delete activity by user/role.

XII. The solution should capture schema/object changes (DDL) activity by user/role.

XIII. The solution should capture manipulation of accounts, roles and privileges (DCL) by user/role.

XIV. The solution be able to monitor activities at new DB interface/ connector created by any user/ system without any manual intervention.

XV. The solution should provide SQL response time for monitoring custom queries.

XVI. The solution should provide response time monitoring for custom queries to allow monitoring unsupported databases.

XVII. The solution should provide database space monitoring for both file group and transaction log (warning threshold, critical threshold as well as file group/log full).

XVIII. The solution should support performance monitoring - capture of DB engine related performance counters as well as threshold alerting.

XIX. The solution must support SQL agent monitoring including failed jobs, long running jobs.

XX. The solution must support database health and settings - check database status (offline, suspect), check database options (auto grow, auto shrink, auto close etc.).

XXI. The solution must support monitoring of replication, DB mirroring and log shipping if applicable.

XXII. The solution must be able to report and check for last recent full database backup and last recent transaction log backup.

XXIII. The solution must monitor for blocking (exceeding duration) and deadlocks

XXIV. The solution must be able to run scripts to perform tests on the database and have the results put into the solution as performance data and or alarms.

XXV. The solution should support discovery of database instances.

XXVI. The solution should support the use of schedules and time filters for database monitoring.

XXVII. The solution should monitor privileged users and administrator activities.

XXVIII. The solution should have an option to upgrade to block privileged users' activity if required.

XXIX. The solution should monitor 100% DB traffic for all DB violation and attacks even if the traffic is not being audited.

XXX. Solution shall have capability to segregate public subnet/networks and private subnet/networks.

3.12. Managed Threat Detection Service:

i. Continuously monitor for malicious or unauthorized behaviour to help protect account and workloads. The service should also detect potentially compromised instances or reconnaissance by attackers.

ii. Threat detection service should be able to generate actionable alerts.

iii. Threat detection service should support integration with event management and workflow systems.

3.13. Web Application Firewall:

i. WAF n shall be able to protect application from vulnerabilities specified in OWASP publications.

ii. WAF shall support monitoring and blocking any malicious HTTP/S traffic traveling to the application.

iii. WAF shall inspect and monitor application and APIs and shall protect it from web exploits.

iv. WAF shall be able to protect the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

v. WAF should be able to give us control over which traffic to allow or block the web application by defining customizable web security rules.

vi. WAF should be able to deploy new rules immediately.

vii. WAF should support API based operations to automate the creation, deployment, and maintenance of web security rules.

viii. WAF shall have the capability of work in learning mode.

ix. WAF must provide at-least (but not limited to) the following Features and Protections against various attacks:

a) Open Web Application Security Project (OWASP) Top 10 attacks

b) OWASP Top 10 API security

3.14. Next Generation Firewall (NGFW):

i. Cloud infrastructure should be protected with NGFW solution with Stateful Inspection, Intrusion Prevention, Web/URL Filtering, Application Control, DoS, User Authentication, Gateway Antivirus and Sandboxing/ATP solution.

ii. Solution should have capability to protect against Denial of Service (DoS) attacks. Should have flexibility to configure threshold values for different anomalies.

xii. Solution should support SAML integration for Admin authentication and SSL VPN authentication.

xiii. NGFW must support SDN Connectors to Public Cloud vendors dynamic object address creation and updating.

xiv. NGFW should support FQDN-based address objects to resolve dynamic internal servers that can be referred in firewall policies.

xv. NGFW should have well documented and maintained default deployment templates for quick and predictable deployment.

xvi. Cloud infrastructure should be protected from Zero Day Malware.

xvii. NGFW must support pre-populated Licensed copies of Operating systems and applications/ software.

3.15. Identity and Access Management:

i. The solution shall securely manage access to services and resources in the Cloud. Assign specific roles to access different Cloud services.

ii. The solution shall Identify the resources in customer accounts, such as Storage objects or IAM roles, that are shared with an external entity (can be another account, a root user, an IAM user or role, a federated user, cloud service, an anonymous user) to identify unintended access to your resources and data, which is a security risk.

iii. Shall support Identity management for web portal. Add user sign-up, sign-in, and access control to the web portal.

iv. It shall provide Central governance and management across accounts to enforce policies, detect violations

v. Cloud Native solution for IAM shall be used. In case, a native solution is not providing satisfactory services, 3rd party solutions shall be explored.

vi. User authorization i.e., role-based access to services, transactions, and data shall be available.

vii. It shall provide Secure storage of user credentials

viii. Root access of the cloud account shall be with DBN.

ix. Industry best practices shall be followed for access management.

x. The system must have proper security and maintenance facility with Role Based Access Control (RBAC) features for controlling the access rights over the system and over the various functions/ features available for different types of users.

xi. Principle of least privilege shall be adopted to grant only the required set of permissions needed to perform the job.

xii. The server security solution that shall be provisioned by bidder, shall support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with Host Intrusion Prevention System (HIPS), Integrity Monitoring and Recommended scan in single agent for physical, virtual and cloud instances.

xiii. The server security solution shall provide automatic recommendations against existing vulnerabilities, dynamically tuning Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) sensors (e.g. Selecting rules, configuring policies, updating policies, etc.) and provide automatic recommendation for removing assigned policies if vulnerability no longer exists - For Example - If a patch is deployed unwanted signatures shall be un-assigned automatically.

xiv. The server solution shall have an intuitive rule creation and modification interface which shall have the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and solution shall have pre and post execution machine learning and shall have Ransom ware protection in behaviour monitoring.

xv. The server security Host based IPS shall support virtual patching for both known and unknown vulnerabilities.

xvi. Shall support prevention against script-based attacks and Distributed Denial of Services (DDoS) which is used to deliver malware such as ransomware

xvii. The server security solution shall protect against DDoS attack and solution shall have the ability to lock down a computer (prevent all communication) except with management server.

xviii. The server security HIPS solution shall not have the need to provision HIPS rules from the Policy Server as the rules shall be automatically provisioned and recommended according to vulnerabilities.

xix. The server security solution shall support pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.

3.16. System Control and Audit:

i. The system should maintain audit trails, audit logs and transaction logs (what, when, who has changed).

ii. It should enable availability of user wise online audit trails/ logs which should be archived based on user, date, time etc. as part of audit records keeping.

iii. All the edited and deleted (if any) records should be traceable and copy of all records should be kept in the system and which should be available with MIS reporting of the same.

iv. The system should maintain all the instances, audit trails, audit logs and transaction logs (what, when, who has changed).

v. The application shall log all the actions done by individual users with username, date time stamp and the administrator shall be able to generate detailed audit logs and history of the process instance.

vi. It should enable availability of user wise online audit trails/ logs which should be archived based on user, date, time etc. as part of audit records keeping.

vii. All the edited and deleted (if any) records should be traceable and copy of all records should be kept in the system and which should be available with MIS reporting of the same.

3.17. Privacy and Data Security:

i. Data must be encrypted while at rest and in transit. Data should be handled in accordance with appropriate and applicable laws of the country.

ii. Security Monitoring and Control

iii. The security, risk and compliance of the cloud platform must be monitored for potential anomalies and threats with events reported to DBN.

3.18. User Administration:

i. SI shall implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.

ii. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles, which they associated with different user account

iii. Bidder shall implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.

3.19. Security Administration:

i. Appropriately configure the security groups in accordance with the IT Act and MietY guidelines.

ii. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.

iii. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.

iv. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.

v. Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the IT Act and MietY guidelines.

vi. Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Security policies inline to IT Act or MietY guidelines.

3.20. DDoS Solution:

i. Bidder should provide native cloud-based DDoS solutions

ii. Solution should secure from system Cache poisoning, SSL/TLS encrypted, DNS reflection, DNS amplification, DNS Tunnelling, DNS Based exploits, TCP/UDP/ICMP floods, DNS protocol anomalies.

iii. Solution should have Behavioural DoS, challenge response, CAPTCHA approach, Geolocation & IP Reputation for mitigation of flood attacks.

iv. All layer 3, 4, and 7 DoS/DDoS threats including flood/sweep, UDP/DNS/HTTP/TCP/SIP/SYN/ACK/RST/FIN, NBA, 120+ DDoS vectors, application anomaly, dynamic filtering, protocol analysis, source tracking.

v. The solution should be ICSA certified & OS should be EAL or NDPP/NDcPP certified under Common Criteria Program. FIPS 140-2 Levels 3.

vi. The Proposed solution should support high performance, scalable for DNS Security, DDoS, WAF, Anti-Bot features.

vii. Should have inbuilt advance and Hardware accelerated purpose-built TLS stack for Key exchange and bulk inspection; RC4, DES, 3DES, AES-CBC, AES-GCM, AES-GMAC, RSA, ECC, DSA, DH, ECDSA, ECDH, MD5, SHA, SHA2 ciphers with FIPS 140-2 Levels 3.

3.21. Legal Compliance Requirements:

i. Bidder shall meet the ever-evolving security requirements as specified by CERT-In.

ii. All services acquired under this application document including data will be guaranteed to reside in India only, at all times.

iii. No legal frameworks outside Indian Law, shall be applicable to the operation of the service.

iv. Bidder shall be prepared to submit the necessary artefacts and the independent verification within the timeframe

v. Bidder shall not publish or disclose in any manner any information, without the DBN's written consent, the details of any safeguards either designed or developed by bidder under the agreement or otherwise provided by the DBN.

vi. Bidder shall strictly adhere to the privacy safeguards as laid down, from time to time, by the DBN, MeitY, NIC and other appropriate government authorities.

vii. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by bidder, bidder shall afford the state or its nominated agency access to bidder's facilities, installations, technical capabilities, operations, documentation, records, and databases.

viii. If new or unanticipated threats or hazards are discovered by either DBN or bidder or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of CERT-In and the other party.

ix. One-time Migration of current deployment/setup (application, compute, storage, security, network etc.) to the proposed CSP's environment.

x. The selected bidder shall ensure migration of entire existing solution landscape (applications, data, databases, file storage, VMs, content and any other assets) from existing cloud setup to the proposed cloud setup and provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of DBN.

3.22. Migration & Installation Services:

i. Bidder shall perform detail As-Is study of existing application and infrastructure landscape and submit the report.

ii. Bidder in this regard shall be required to submit a migration plan to DBN for migrating the existing application/ workload on its proposed Cloud. Necessary support will be provided by the technical team of the DBN.

iii. Bidder shall be responsible for cloud infrastructure / service deployment, migration,

coordination with application stakeholders, specific troubleshooting or other planning tasks etc. as required by DBN.

iv. Bidder is solely responsible for both transition of the services as well as migration of the VMs, data, content and other assets to the new environment. The migration shall also include the migration of underlying data & files from the current database(s) / storage into the new database(s) / storage on the cloud.

v. It is suggested to use migration tool to migrate the application smoothly and with minimum or zero downtime.

vi. Bidder shall ensure successful deployment and running of the existing solution in the new environment and bidder shall submit documents related to migration.

3.23. Monitoring Performance and Service Levels:

i. Bidder shall provide and implement tools and processes for monitoring the availability of migrated and hosted applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues

ii. Bidder shall ensure monitoring and reviewing the service levels (including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service detecting and reporting service level agreement infringements service level reports, monitoring the service levels and identifying any deviations from the agreed service levels

iii. Bidder shall ensure monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating systems, applications, including API access within the bidder's boundary through tools and share the reports on monthly basis to the DBN

iv. Native solutions shall be used for monitoring and performance dashboards.

3.24. Usage Reporting and Billing Management:

i. Bidder shall track system usage, the same shall be submitted to DBN on monthly basis and at the end of every quarter as part of documentary evidence.

ii. Bidder shall undertake monitoring, managing and administering the monetary terms of SLAs and other billing related aspects.

iii. Backup, restore, disaster management and business continuity

iv. Bidder shall configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy laid by bidder and finalized in consultation with DBN.

v. Bidder shall ensure daily incremental and weekly full backup taken for all services like virtual machines, storage etc. The backup shall be tested on a half yearly basis. However, DBN reserves the right to define / update the backup strategy for different applications and SI shall configure the backup policies as per requirements.

vi. Bidder shall submit a well-defined plan for backup and recovery including processes and procedures etc. related to recovery or continuation of services.

3.25. Resource Management:

i. Bidder shall adequately size the necessary compute, storage and other cloud services required, building the redundancy wherever necessary into the architecture and load balancing to meet the service levels as laid in the procurement document

ii. While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provided in the procurement document, subsequently, it is expected that the bidder , based on the growth in the user load (peak and non-peak periods; year-on-year increase), shall scale up or scale down the compute, memory, and storage as per the performance requirements needed to run all the DBN's applications in a seamless manner and meet the SLAs using the auto-scaling features.

iii. In addition to auto-scaling, for any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements

iv. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits must be changed) must be carried out with prior approval by the DBN. The bidder shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.

3.26. Helpdesk and Manpower:

Bidder shall setup helpdesk for technical query resolution and ensure that the dedicated team of support staff are available 24/7 for such resolution of the queries. Bidder shall appoint a Project Manager who shall be point of contact for the DBN and should be placed at DBN Premises till the project Go-Live date. Details of the manpower shall be mentioned in RFP response as per Annexure R of this RFP Document.

3.27. Exit Management / Transition-Out Services:

Continuity and performance of the services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of DBN. It is the prime responsibility of bidder to ensure continuity of service at all times of the agreement including exit management period and in no way any facility/service shall be affected/degraded. Responsibilities of bidder with respect to exit management / transition-out services include:

i. Providing a comprehensive exit management plan

ii. Provide necessary handholding and transition support for any other bidder to ensure the continuity and performance of the services to the complete satisfaction of the DBN.

iii. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date

iv. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest with the DBN only. The Bidder

shall take utmost care in maintaining security, confidentiality and backup of all including this data.

v. Ensure that all the documentation required by DBN for smooth transition including configuration history are and all such logs are handed over to DBN during the exit management process.

vi. Upon the determination of the Agreement with DBN or in the event of pre-mature termination, it shall be the responsibility of the Bidder not to delete any data of for a period of 45 days after such determination or pre-mature termination of the Agreement, without the express approval of DBN. DBN shall pay for the cost for retaining the data as per the prices discovered in the commercial bid after the above referred period of 45 days, if required to retain the data.

vii. Once the exit process is completed, remove the DBNs data, content and other assets from the cloud environment and certify that the VM, Content and data deletion to DBN

viii. There shall not be any additional costs associated with the Exit / Transition-out process other than the cost of cloud services utilized for such transition. The managed services cost to support the exit management / transition shall be factored in the commercial bid of bidder.

ix. Train and transfer the knowledge to the DBN team to ensure similar continuity and performance of the Services post expiry of the Agreement.

3.28. Termination of the Contract:

Administrator, DBN reserves the right to suspend any of the services and/or terminate the agreement/contract in one or more of the following circumstances by giving 30 days' notice in writing:

a) In case, the overall penalty/deduction for the selected bidder exceeds 10% of the contract value **3 times consecutively.**

b) The selected bidder has failed to commence the Services as per the timelines of the RFP. If staffing personnel and/or services as per the scope of work under the contract with DBN is not found satisfactory by DBN.

c) Termination for Insolvency, Dissolution etc - Administrator, DBN may at any time terminate the contract by giving written notice to the selected/ Agency without compensation to the selected/ Agency, if the selected/ Agency becomes bankrupt or otherwise insolvent or in case of dissolution of firm or winding up of company, provided that such termination will not prejudice or effect any right of action or remedy which has accrued thereafter to DBN.

d) Termination for Default: Administrator, DBN may without prejudice to any other remedy for breach of contract, (including forfeiture of security deposit, Performance Bank Guarantee) by written notice of default sent to the Agency, terminate the contract in whole or in part after sending a notice to the Agency in this regard.

i. If the Agency fails to accept the Work Order(s).

ii. If the Agency fails to deliver services within the time-period specified in the Work Orders or during any extension thereof granted by DBN.
iii. If the Agency fails to meet any other terms and conditions under the contract.

e) **Termination for Convenience:** Administrator, DBN may by written notice, sent to the selected MSP, terminate the work order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination will specify that termination is for DBN's convenience, the extent to which performance of work under the work-order and/or the contract is terminated and the date upon which such termination becomes effective. Administrator, DBN reserves the right to cancel the remaining part and pay to the selected MSP an agreed amount for partially completed Services.
f) The selected bidder has neglected or failed to observe and perform all or any of the term's acts, matters or things under this Contract to be observed and performed by it. The selected bidder has acted in any manner to the detrimental interest, reputation, dignity, name, or prestige of DBN.

3.29. Enterprise Management System:

i. In addition to the hardware and software requirements of this implementation, bidder shall also implement and maintain an Enterprise Management System (EMS). The EMS should be able to support the proposed hardware and software components at Cloud Platform over the tenure of the contract. The EMS should be capable of providing early warning signals to bidder/Dept on the solution performance issues, and future infrastructure capacity augmentation.

ii. Bidder is required to supply, customize, implement, rollout, test, train, and maintain the EMS application and hardware at the Cloud Platform as per the requirements of this RFP. Bidder is expected to provide and implement an EMS encompassing the following functions:

a) Configuration Management
b) Fault Management
c) Incident, Problem and Change Management
d) Asset Management
e) Remote Control
f) SLA management & monitoring
g) Performance management
h) Monitoring Backup and Management
i) Event Management
j) Server, storage and other infrastructure management
k) Monitor network components of the LAN & WAN
l) Network Link Monitoring

iii. The system should be able to generate user friendly Graphical Reports, Trends, Dashboards, etc. in customised and standard form.

iv. The system should provide error logging facility. The system should have ability to redo/ rollback a transaction after recovery from software/ hardware failure to ensure data integrity.

v. The system should restrict users from deleting data directly unless authorized to do so. In case of authorized users also, only soft delete facility would be available.

vi. The system should allow multiple users to access the same module simultaneously.

vii. The system should display data according to user profile/ access rights.

viii. The system should provide functionality to users in generating reports on their own without having knowledge about technical programming.

ix. Any document or report should be previewed before printing.

x. The system should notify users automatically after report is generated.

xi. The system should have a mechanism for resetting and emailing the new password to the users registered email ID, in case one forgets his password

xii. The system should provide facility to block or unblock any user access

4. Instructions to the Bidder:

4.1 General Instructions:

i. While every effort has been made to provide comprehensive and accurate information about requirements and specifications, bidders must form their own conclusions about the solution needed to meet the requirements specified in the RFP.

ii. The requirements of the RFP shall prevail over any information in the Bid. However, all information supplied by the successful bidder will be treated as contractually binding on the bidder.

iii. This RFP supersedes and replaces any previous public documentation and communications, and bidders should place no reliance on such communications.

iv. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of DBN.

v. DBN may cancel this bid process, at any time prior to a formal written contract, being executed by or on behalf of DBN without having an obligation to describe the reasons for the same.

vi. This RFP document is non-transferable.

vii. The RFP should not be used to market the bidder's product or services.

4.2 Pre-Bid Meeting:

i. A pre-bid meeting to discuss and resolve the queries of the interested bidder shall be conducted as per details mentioned in Schedule of Events sections of this RFP

ii. Details of the attendees shall be shared by the bidder in accordance with the format given in Annexure-L

4.3 Availability of RFP Document:

i. The complete Bidding documents are available at GeM (Govt. e-market place) portal https://www.gem.gov.in.
ii. Bidders can obtain the RFP from the website and submit their response. It is the responsibility of the bidder to check the eligibility criteria.
iii. Bidders shall take appropriate care to visit the website to get updated about the addendums / corrigendum published by DBN, which would form part of the bid documents.

4.4 Bid Security & EMD:

The Bidders shall submit, along with their bids, a Bid security declaration as per the format specified in **Annexure E** of this RFP and shall be liable as per the declaration.

The Bidder shall furnish, as part of its bid, a bid security through Account Payee Demand Draft/Bank Guarantee/ Surety Bond from any of the commercial banks drawn in favour of "Digital Bharat Nidhi, HQ, Department of Telecommunications, Ministry of Communications, New Delhi" payable at Delhi for an amount of Rs.6,00,000 (Rs. Five Lakhs Only). Bid security should be valid for a period of 180 days from the date of submission of the bid. BG can be given against EMD as per **Annexure-E** of the RFP. Exemption from submission of EMD is accepted subject to submission of requisite and valid documents as per Govt. of India guidelines. The firms registered under MSE/ startups are exempted from submitting the Earnest Money Deposit). If a Bidder falls under MSE, then a copy of the MSE registration certificate under the relevant category must be provided to DBN along with the proposal. Exemption will be provided subject to submission of requisite and valid documents as per Govt. of India guidelines. Exemption from EMD will be dealt in accordance with the relevant provisions of GeM-GTC-2024.

Bidders claiming exemption of EMD under rule 170 of GFR are however required to submit a signed Bid security declaration (as enclosed) accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for the period of 24 months from being eligible to submit Bids for tenders with DBN. Scanned copy of the signed documents related to exemption of EMD and related supporting documents shall be submitted online at the time of submission of bid proposal and hard copy of original documents along with Bid Security Declaration, shall be submitted at the DBN HQ before last date of submission of proposals. The proposals of such Bidders whose supporting documents regarding the exemption of bid security is not received by the bidder before the last date of submission, will automatically be rejected.

EMD shall be forfeited (or in case BSD is permitted, the declaration) shall be enforced from the date of such decision) if the Bidde(s) breaches any of the following obligation(s) under the RFP:

(a) withdraws or amends his Proposal or impairs or derogates from the Proposal in any respect within the period of validity of its Proposal; or
(b) after having been notified within the period of Proposal validity of the acceptance of his Proposal by DBN:

(i) refuses to or fails to submit the original documents for scrutiny or the required Performance Security within the stipulated time as per the RFP document's conditions.

(ii) fails or refuses to sign the contract.

EMD furnished by all unsuccessful bidders will be returned back to respective bidders as early as possible after the expiry date of validity of their offer but not later than 30 days of award of the contract.

4.5 Performance Bank Guarantee:

Successful bidder shall furnish performance security to DBN for an amount equal to 5% of the value of total bid, as per format specified in Annexure F within 14 days from the date of issue of Advance Purchase Order (APO) issued by DBN.

The Performance Security Bond shall be in the form of Bank Guarantee or insurance security bond issued by a nationalized / scheduled bank or insurance company approved by IRDA and in the form provided in Annexure-F of this Bid Document. Validity of such Bank Guarantee shall be 3 years. Validity shall be got extended by the Successful Bidder as and when required to cover the periods of extension and shall be valid for six months beyond the dates of such extensions.

The Performance Security Bond will be discharged by DBN after completion of Bidder's performance obligations including any warranty obligations under the Agreement.

4.6 Bid Preparation Costs:

i. The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal and in providing any additional information required by DBN to facilitate the evaluation process.
ii. DBN will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.
iii. This RFP does not commit DBN to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award or for preparing this RFP.
iv. All materials submitted by the bidder will become the property of DBN and may be returned completely at its sole discretion.

4.7 Bidder Presentation:

Bidders are required to make a presentation before the selection committee of DBN. Following must be included in the presentation apart from other details:

i. Demonstration of Bidder's understanding of the project requirement.
ii. Plan for implementation/Risk mitigation and adherence to SLA.
iii. Migration and Backup Strategy.
iv. High Availability and Security Plan.
v. Challenges likely to be encountered and solution proposed.
vi. Helpdesk Solution proposed

4.8 Consortium and Sub-Contracting:

Consortium and Sub-Contracting are not allowed in this bid.

4.9 Debarment from Bidding:

i. The bidder shall be debarred if they have been convicted of an offence –
   a) Under the Prevention of Corruption Act, 1988; or
   b) The Indian Penal Code, 1860/ Bhartiya Nyay Samhita 2023 or any other law for the time being in force, for causing any loss of life or property or causing a threat to public health as part of execution of a public procurement contract.

ii. A bidder debarred under Section 1.7 (1) (a) above or any successor of the bidder shall not be eligible to participate in a procurement process of any procuring entity for a period not exceeding three years commencing from the date of debarment.

4.10 Authorized Signatory and Authentication of Bids:

The "Authorized Signatory" shall mean the one who has signed the Bid document. The authorized signatory may be either the head of the organization or the duly Authorized Representative of the Bidding organization, in which case the Bidder shall submit a power of attorney authorizing the person to be authorized signatory or a copy of board resolution as per **Annexure D** (Power of Attorney). The power of attorney/ board resolution of the Bidder must be submitted along with the proposal.

4.11 Language:

The Proposal must be filled by the bidders in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is required and should be duly attested by the Bidder. For purposes of interpretation of the documents, the English translation shall govern.

4.12 Complete and Compliant Responses:

i. Bidders are advised to study all instructions, forms, requirements and other information in the RFP document carefully. Submission of the proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

ii. The response to this RFP should be full and complete in all respects. Failure to comply with the requirements of this clause may render the Proposal non-compliant and the Proposal may be rejected. Bidders must-
   a. Include all documentation specified in this RFP.
   b. Follow the format of this RFP and respond to each element in the order as set out in this RFP.
   c. Comply with all requirements as set out in this RFP.

4.13 Late Bids:

i. All Bidders are required to submit their bids (complete in all respects) within the time and date as specified in RFP event schedule. The Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained. The

Bids submitted by telex/telegram/fax/e-mail/manually etc. shall not be considered. No correspondence will be entertained on this matter DBN shall not be responsible for any delay or non-receipt/non-delivery of the documents. No further correspondence on the subject will be entertained. DBN reserves the right to modify and amend any of the above-stipulated condition/criteria depending upon project priorities vis-à-vis urgent commitments.

ii. Given that the bid submission has to be made electronically on GeM portal, it is advised that the Bidder takes all necessary precaution for the same, including submitting the Bid well in advance to avoid any last-minute hassles. DBN shall not entertain any bids which could not be submitted properly for whatsoever reasons.

iii. DBN may, in exceptional circumstances and at its discretion, extend the deadline for submission of proposals by issuing an addendum/corrigendum (on GeM portal) or by intimating all bidders, in writing or through e-mail. In such case all rights and obligations of DBN and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

4.14 Proposal Submission Format:

a. The entire proposal shall be submitted as per the format specified in this RFP and any deviation may result in the rejection of the RFP proposal. Refer **Annexure A** (Pre-Qualification proposal format & **Annexure N, Annexure O** for Commercial proposal format) for the format for Proposal Submission.
b. A two staged bid system will be followed for this RFP with Quality cum Cost Based Selection criteria. The two bids to be submitted by bidders on GeM are –
   - Technical Bid and
   - Commercial Bid
c. The bid response of the Bidder to be submitted and uploaded on the GeM portal against this RFP.
d. The bids are to be submitted electronically on GeM on or before the last date of proposal submission. Bids received in any other form will not be accepted and may lead to rejection of the bid.
e. This RFP process will be administered through the GeM portal. The bidders are required to submit soft copies of their bids electronically on the GeM Portal, by the officer duly authorized to submit the bid. The bidders are required to enrol on the GeM portal. Detailed instructions, FAQ, call centre number details are mentioned on GeM (please visit- www.gem.gov.in). For convenience, bidders are thus advised to go through such instructions (as published on GeM) and take necessary assistance through the GeM call centre (if required) in order to properly submit their bids on time.
f. The Bidder should take into account any corrigendum to this RFP document that may have been published before submitting their Proposals
g. The Proposal is to be submitted in three (3) covers on GeM as mentioned below

S. No.	Bid covers	Bid submission
1	Bid Security Declaration	Scanned copy to be uploaded on GeM and original to be submitted to DBN office before due date of

		submission of bid as mentioned in Schedule of Events on Page 2 of this RFP
2	Technical Bid	To be uploaded on GeM
3	Commercial bid	To be uploaded on GeM

h. The contents of bid shall be as under:

S. No.	Document Name	Contents
1	Bid Security Declaration	a. Scan copy of Bid Security Declaration as per **Annexure E** (Bid Security Declaration)- (Original Bid Security Declaration to be submitted in a sealed cover at DBN office before due date of submission of bid as mentioned in Schedule of Events on Page 2 of this RFP). b. Power of attorney/Board Resolution as per **Annexure D** (Power of Attorney) – (Original signed Power of attorney/Board Resolution to be submitted in a sealed cover at DBN before due date of submission of bid as mentioned in Schedule of Events on Page 2 of this RFP).
2	Technical Bid	a. Pre-Qualification Proposal as per **Annexure A** (Pre-Qualification Proposal Format) along with the specified documents/Forms. b. Checklist of all documents submitted.
3	Commercial bid	c. Commercial Proposal as per the required supporting documents/forms specified at **Annexure N, Annexure** O (Commercial Proposal Format). d. Check list of all documents submitted

i. The response to pre-qualification bid and commercial bid (as mentioned in the previous paragraph) should be uploaded in separate folders on the GeM portal.

j. Please note that prices must not be indicated in the pre-qualification bid and must only be indicated in the commercial bid. In case any bidder submits prices or any other commercial information in its pre- qualification bid then the bids of such bidders will be summarily rejected by DBN.

k. The pre-qualification bid and commercial bid should be complete documents and should be in separate single PDF documents. All the pages of the bid must be sequentially numbered and must contain the list of contents with page numbers. Bidders are required to submit all details as per the formats given in the RFP document only. Any deficiency in documentation may result in the rejection of the bid at the sole discretion of DBN.

l. Original Bid Security Declaration, Power of attorney/Board resolution and signed integrity pact as per Annexure S, is required to be submitted manually at DBN's office in a sealed cover and a scan copy of Bid Security Declaration, Power of attorney/Board resolution and signed integrity

pact needs to be uploaded on GeM by the bidders. While submitting the original Bid Security Declaration, Power of attorney/Board resolution and signed integrity pact, it should be placed in a sealed cover and the envelope be super scribed as "Bid Security Declaration, Power of attorney/Board resolution and Integrity pact for RFP for selection of MSP for Digital Bharat Nidhi. Original Bid Security Declaration, Power of attorney/Board resolution and signed integrity pact must be submitted on or before the last date of submission at the following address:

Sh. Sathish Kumar MC
Deputy Administrator, Digital Bharat Nidhi,
Room no. 1103, Sanchar Bhawan,
Ashoka Road
New Delhi - 110011

4.15 Amendment of the RFP:

At any time prior to the deadline for submission of the proposals, DBN, for any reason, may modify the RFP by amendment/ corrigendum and it shall publish the same on GeM portal. Such amendments shall be binding on the Bidders. Bidders are requested to regularly visit GeM portal and check for themselves regarding any addendum/corrigendum issued to the RFP. DBN shall, in no way, be responsible for any lapse of information on part of the concerned bidder(s) for non-checking the GeM portal for RFP related updates/information.

In this case, all rights and obligations of DBN and the Bidder(s), previously subject to original deadline shall then be subject to the new deadline for the RFP submission

4.16 Bid Validity:

Bids must remain valid up to 180 (One Hundred & Eighty) days from the last date of submission of the Bids. DBN may request the Bidder(s) for an extension of the period of validity of the bids which may suitably be extended post such requests by the bidders.

4.17 Right to the Content of Proposal:

All bids and accompanying documentation of the bid proposal will become the property of DBN and will not be returned after opening of the bid proposals. DBN is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the bidders. DBN shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

4.18 Disqualification:

The Proposal is liable to be disqualified in, inter alia, any of the following cases or in case the Bidder fails to meet the bidding requirements as indicated in this RFP:

- Bid not submitted in accordance with the terms, procedure and formats prescribed in this document or treated as non-conforming proposal;

- During validity of the bid, or its extended period, if any, the Bidder increases its quoted price after the submission of the bid;
- The Bidder's Proposal is conditional and has deviations from the terms and conditions of RFP;
- The Proposal is received in an incomplete form;
- The Proposal is received after the due date and time;
- The Proposal is not accompanied by all the requisite documents;
- The Proposal is submitted without the bid security declaration as per the format specified in the RFP;
- The information submitted in the proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period, if any;
- The Bidder(s) has an obligation and shall ensure that its Experts and Subconsultants shall have an obligation to disclose any actual or potential conflict that impacts their capacity to serve the best interest of DBN, or that may reasonably be perceived as having this effect. Failure to disclose said situations may lead to the disqualification of the Bidder and/ or the termination of the Contract.
- If the Bidder(s), before award or during execution, has committed a transgression through a violation of its commitments or in any other form such as to put their reliability or credibility in question, then DBN is entitled to disqualify the Bidder(s) from the bidding process or service as well as take appropriate action as per the procedure outlined in the RFP document.
- The commercial proposal is enclosed within the prequalification bid or any other proposal or vice-versa;

4.19 Right to Intellectual Property and Confidentiality:

Information relating to the examination, clarification and any other purpose of the RFP shall not be disclosed to any persons not officially concerned with such process until the process is over. Undue use of confidential information related to the process by any firm may result in rejection of its proposal

1) The RFP Document and associated correspondence are subject to copyright laws and shall always remain the property of DBN and must not be shared with third parties or reproduced, whether in whole or part, without DBN's prior written consent.
2) However, Bidder(s) may share these to prepare and submit their Proposals with their employees, Sub-consultant(s) or holding Company after obtaining an undertaking of confidentiality similar to that imposed on the Bidder.
3) This condition shall also apply to Bidder(s) who do not submit a Proposal after downloading it or are not awarded a contract.
4) The obligation of the Bidder(s) under sub-clauses above, however, shall not apply to information that:
   a) now or hereafter is or enters the public domain through no fault of Bidder(s);
   b) is legally possessed by Bidder(s) at the relevant time and was not previously obtained, directly or indirectly, from the Procuring Entity; or
   c) otherwise lawfully becomes available to Bidder(s) from a third party with no obligation of confidentiality.

The provisions of this clause shall survive completion or termination for whatever reason of the Procurement Process or the contract.

4.20 Fraud and Corrupt Practices:

i. The Bidders and their respective officers, employees, agents and advisors shall observe the highest standard of ethics during the selection process. Notwithstanding anything to the contrary contained in this RFP, DBN may reject a proposal without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the selection process. In such an event, DBN may, without prejudice to it's any other rights or remedies, forfeit and appropriate the PBG.

ii. Without prejudice to the rights of DBN here in above and the rights and remedies which DBN may have under the Agreement, if a Bidder is found by DBN to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the selection process, or after the issue of the Letter of Award (LOA) or the execution of the Agreement, such Bidder shall not be eligible to participate in any tender or RFP issued by DBN during a period of 3 years from the date such Bidder is found by DBN to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

iii. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

a) "Corrupt Practice" means

i. The offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the selection process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of DBN who is or has been associated in any manner, directly or indirectly with the selection process or the LOA or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of DBN shall be deemed to constitute influencing the actions of a person connected with the selection process); or

ii. Save as provided herein, engaging in any manner whatsoever, whether during the selection process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/adviser of DBN in relation to any matter concerning the Project;

b) "Fraudulent Practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the selection process;

c) "Coercive Practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the selection process.

d) "Undesirable Practice" means

i. Establishing contact with any person connected with or employed or engaged by DBN with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the selection process; or

ii. Having a Conflict of Interest

e) "Restrictive Practice" means forming a cartel or arriving at any understanding or arrangement among the Bidders with the objective of restricting or manipulating a full and fair competition in the selection process.

4.21 Right to Terminate the Process:

i. DBN may terminate the RFP process at any time and without assigning any reason. DBN makes no commitments, express or implied, that this process will result in a business transaction with anyone.

ii. This RFP does not constitute an offer by DBN. The bidder's participation in this process may result in short listing the bidders.

4.22 Conflict of Interest:

i. The Bidder shall not have a conflict of interest that may affect the selection process (the "Conflict of Interest"). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, DBN shall forfeit and appropriate the PBG, if available, as mutually agreed genuine pre-estimated compensation and damages payable to DBN for, inter alia, the time, cost and effort of DBN including consideration of such Bidder's Proposal, without prejudice to any other right or remedy that may be available to DBN hereunder or otherwise.

ii. DBN requires that bidders provide professional, objective, and impartial services and at all times hold DBN's interests' paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The bidders shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of DBN.

iii. Without limiting the generality of the above, the Bidder shall be deemed to have a Conflict of Interest affecting the Selection Process, if:

a) The Bidder, or Associates (or any constituent thereof) have common controlling shareholders or other ownership interest;

b) Such Bidder or its Associate receives or has received any direct or indirect subsidy or grant from any other Bidder or its Associate; or

c) Such Bidder has a relationship with another Bidder, directly or through common third parties, that puts them in a position to have access to each other's information about, or to influence the Proposal of either or each of the other Bidder; or

d) There is a conflict among this and other assignments of the bidder.

e) Bidder (including its personnel and other members, if any) and any subsidiaries or entities controlled by such Bidder or having common controlling shareholders. The duties of the bidders will depend on the circumstances of each case. While providing services to DBN for this particular assignment, the bidders shall not take up any assignment that by its nature will result in conflict with the present assignment; or

f) A firm hired to provide similar services for the preparation or implementation of a project, and its members or Associates, will be disqualified from subsequently providing goods or works or services related to the same project;

iv. A Bidder eventually appointed to provide services for this Project shall be disqualified from subsequently providing goods or services related to the same Project and any breach of this obligation shall be construed as Conflict of Interest; provided that the restriction herein shall not apply after a period of 24 months from the completion of this assignment; provided further that this restriction shall not apply to services performed for DBN in continuation of this project or to any subsequent services performed for DBN where the conflict of interest situation does not arise.

v. In the event that the bidder, its Associates or affiliates are auditors or financial advisors to any of the Bidders for the Project, they shall make a disclosure to DBN as soon as any potential conflict comes to their notice but in no case later than 7 (seven) days from the receipt of such proposals and any breach of this obligation of disclosure shall be construed as Conflict of Interest. DBN shall, upon being notified by the bidder under this Clause, decide whether it wishes to terminate this Consultancy or otherwise, and convey its decision to the bidder within a period not exceeding 15 (fifteen) days.

4.23 DBN's right to accept or reject any or all proposals:

Administrator, DBN reserves the right to accept or reject any proposal, and to annul the tendering process /Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for Purchaser action.

5 RFP Evaluation Process:

To establish the bidder's competency and capabilities, it is proposed that the evaluation of the bids will be done in two stages as mentioned below:

Stage-1:

- Evaluation of Pre-Qualification Proposal to establish the Eligibility Claim.
- Evaluation of Technical Proposal

Stage-2:

- Evaluation of Financial Proposal
  - ***On each of these parameters, the bidders would be required to meet the qualification/ evaluation criteria as detailed in subsequent sections.***
- All those bids meeting the Pre-Qualification Criteria would progress to the next level of evaluation i.e. Technical Bid Evaluation.
- Post technical evaluations, only the technically qualified bids would progress to next level of evaluation i.e. Financial Bid Evaluation.

5.1 Pre-Qualification Criteria – Bidder:

S. No.	Criteria	Documentary Evidence
1	**Legal Entity:** Bidder rmust be incorporated and registered in India under the Indian Companies Act 1956 as amended by the companies act 2013 or Indian Partnership Act 1932, LLP registered under LLP Act 2008 or Joint Venture or consortium partner and should have been operational in India for minimum of 3 consecutive years	a. Latest Certification of Incorporation/ Latest Registration Certificate/certificate of Joint Venture/Consortium Partnership Deed. b. GST registration
2	**Financials:** Bidder must have an average annual turnover of minimum of INR 10 crores over the last three financial years (FY 2021-22 and 2022-23 & 2023-24) from providing Cloud infrastructure & management services Bidder should have positive net worth in each of the last three financial years (FY 2021-22 and 2022-23 & 2023-24)	a. Extracts from the audited Balance sheet for the last three financial years (FY 2021-22 and 2022-23 & 2023-24). The relevant sections must be clearly highlighted b. Certificate from the Statutory Auditor on turnover details & net worth over the last three financial years (FY 2021-22 and 2022-23 & 2023-24)

3.	**Technical Capability:** Bidder should have managed or managing the IT infrastructure for Cloud services for at least 3 Cloud Solution Projects in Central Government or State Government or Public Sector enterprise during the last three financial years. 1) Three projects of minimum value of 4.00 Crore each having scope of Application and Data Migration Services to Cloud (At least one project should be of Migration from On-Prem Physical Infrastructure to Cloud, setting up & hosting of IT infrastructure & systems at Cloud) and providing managed services Or 2)Four projects of minimum value of 3.00 Crore each having scope of Application and Data Migration Services to Cloud (At least one project should be of Migration from on prem Physical Infrastructure to Cloud, setting up & hosting of IT infrastructure & systems at Cloud) and providing managed services Or 3) Five projects, of minimum value of 2.50 Crore each having scope of Application and Data Migration Services to Cloud (At least one project should be of Migration from on prem Physical Infrastructure to Cloud, setting up & hosting of IT infrastructure & systems at Cloud) and providing managed services Note: Projects covering solution & infrastructure provided for self-use shall not be considered	a. Work Order and / or Signed Contract (And) b. For Completed Projects - Client Completion Certificate or Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead OR Copies of payments received, signed by the Statutory Auditor/Company Secretary of the Bidders or any other document certifying the status of the project OR For on-going projects - Satisfactory Work in Progress Certificate (certifying that the requisite services are being provided for at least three months), from the Client

4.	**Certifications:** Bidder should possess following mandatory certifications: • ISO 27001:2013/2022 for Information Security Management System • ISO 9001:2008 / ISO 9001:2015 for Quality Management System • ISO 20000:2011 for IT Service Management	Copies of valid certificates as on application submission date
5.	**Self - Declaration on Non-Blacklisting:** Bidder should not have been blacklisted / debarred by any Govt of India/State Government entity or any PSU in India as on the date of bid submission	Undertaking on Company's Letterhead, duly signed and stamped and to be counter signed by Bidder's Country Head
6.	**Manpower strength:** The bidder must have strength of at least 15 IT Professionals (data centre /networking/system administration/ cloud services professional's/cloud security experts) on their payroll as on date of submission. At least 5 of these professionals must have experience of minimum 7 years in maintenance of cloud solution/ DR Management / virtual server administration/system administration, Virtualization, security, database etc. along with relevant certifications	Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the application as per the requirement.
7.	**MSP-CSP Partnership:** The MSP must be an authorized partner of one or more MeitY empanelled CSP.	Duly signed Authorization letter of MeitY empanelled CSP, on CSPs letter head, whose services are provided by MSP

5.2 Pre-Qualification Criteria – CSP:

Each eligible CSP should possess all the following eligibility qualification criteria. Responses not meeting the minimum qualification criteria shall be rejected.

Sl No.	Mandatory Criteria	Documentary Evidence
1	The Cloud Service Provider (CSP) must be empanelled with the Ministry of Electronics & Information and Technology (MeitY), Government of India.	Undertaking on CSP letterhead confirming the clause and copy of Valid MeitY Empanelment Certificate
2	Cloud Service Provider must have expereince of executing at least 5 projects with the Government of India/State Government/PSU in the last three financial years (FY 2021-22 and 2022-23 & 2023-24) incompassing the requirement mentioned in this RFP document.	a. Work Order and / or Signed Contract (And) b. For Completed Projects - Client Completion Certificate or Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead OR Copies of payments received, signed by the Statutory Auditor/Company Secretary of the Bidders or any other document certifying the status of the project OR For on-going projects - Satisfactory Work in Progress Certificate (certifying that the requisite services are being provided for at least three months), from the Client
3	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3	Self-declaration from the Authorized signatory of the CSP on their letterhead or Public Link

Important Note:

a. The MSP must quote solution with any one MeitY empanelled CSP only. The MSP must submit the Authorization letter from the CSP as part of Pre- qualification. Since the MSP will be evaluated on the proposed solution; they are not allowed to change the CSP post bid submission.

b. If the selected CSP cease to operate in India or is blacklisted by the government; MSP and DBN shall mutually decide on any other CSP and the scope for migration will be with the

MSP at a mutually agreed rate between DBN and the MSP. DBN may also go for tendering process to finalise the migration cost.

c. Bidder and Cloud Service Provider (CSP) may be a single entity. In such case, Bidder shall qualify for both the Criteria i.e. “Pre-Qualification Criteria for Bidder” and “Eligibility Criteria for the CSP”.
d. Bidder and Cloud Service Provider (CSP) may be different entity. In such case, Bidder shall qualify for “Pre-Qualification Criteria for Bidder” and “Eligibility Criteria for the CSP”.
e. In any of the cases above, Bidder shall be solely liable to and responsible for all obligations towards the performance of works/services/adherence to SLAs under the contract

5.3 Technical Evaluation Criteria:

i. Bidders that satisfy the pre-qualification criteria will be considered for the Technical Evaluation.
ii. The Committee shall evaluate the technical proposal to verify the compliance against the requirements in this Application Document. The bidder shall submit the Technical Proposal in the form at **Annexure G.**
iii. The technical proposal should address all the areas / sections as specified in the application document and should contain a detailed description of how the Bidder will provide the required services outlined in this application document. It should articulate in detail, as to how the Bidder’s Technical Solution meets the requirements specified in the application document. The technical proposal must not contain any pricing information.

The technical proposal shall be evaluated on the basis of following table:

Sl No.	Parameter	Evaluation Criteria	Max Marks	Documents Required
1	Average Annual Turnover- Bidder must have an average annual turnover of minimum of INR 10 crores over the last three financial years (FY 2021-22 and 2022-23 & 2023-24) from providing Cloud infrastructure & management services	>INR 10 Crore ≤ 12 Cr- 5 Marks >INR 12 Crore ≤ 15 Cr- 8 Marks >INR 15 Cr- 10 Marks	10	Extracts from the audited Balance sheet and Profit & Loss for the last three financial years (FY 2021-22 and 2022-23 & 2023-24) (and) Certificate from the Statutory Auditor on turnover details & net worth over the last three financial years (FY 2021-22 and 2022-23 & 2023-24)

<table>
<tr><th>Sl No.</th><th>Parameter</th><th>Evaluation Criteria</th><th>Max Marks</th><th>Documents Required</th></tr>
<tr><td>2</td><td>Bidder's Relevant Experience- Bidder should have experience of managing the IT infrastructure for Cloud services for at least 3 Cloud Solution Projects in Central Government or State Government or Public Sector Enterprise during the last three financial years.</td><td>
<table>
<tr><th rowspan="2">No of Projects</th><th colspan="3">Individual Project Value (INR Cr)</th></tr>
<tr><th>>=4</th><th>3-4</th><th>2.5-3</th></tr>
<tr><td>3</td><td>9</td><td>6</td><td>3</td></tr>
<tr><td>4</td><td>12</td><td>8</td><td>4</td></tr>
<tr><td>5</td><td>15</td><td>10</td><td>5</td></tr>
<tr><td>5+</td><td>20</td><td>13</td><td>6</td></tr>
</table>
One (1) extra mark shall be awarded for each project using latest technologies such as AI, ML, IoT etc. maximum up to Five (5) Marks</td><td>25</td><td>Work orders or completion certificates from government/PSU projects
Detailed case studies highlighting similar cloud projects, along with client references</td></tr>
<tr><td>3</td><td>Experience of Manpower strength:
The bidder must have strength of at least 15 IT Professionals (data centre /networking/system administration/ cloud services professional's and cloud security experts) on their payroll as on date of submission.
At least 5 of these professionals must have experience of minimum 7 years in maintenance of cloud solution/ DR Management / virtual server administration/system administration, Virtualization, security, database etc. along with relevant certifications</td><td>
<table>
<tr><th></th><th colspan="3">7+ Years Experience CV</th></tr>
<tr><td>CV Count</td><td>15</td><td>10</td><td>5</td></tr>
<tr><td>Marks</td><td>10</td><td>8</td><td>5</td></tr>
</table>
One (1) extra mark shall be awarded for each resource having experience of more than 15 years maximum up to Five (5) Marks</td><td>15</td><td>Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the application as per the requirement</td></tr>
<tr><td>4</td><td>Solution Proposed</td><td>Unique Value Proposition and technical architecture proposed (5 Marks)

Homogeneity of Proposed Services (5 Marks)</td><td>10</td><td>Relevant certificate/Public Document reference</td></tr>
</table>

Sl No.	Parameter	Evaluation Criteria	Max Marks	Documents Required
5	Experience in Data Migration	Projects executed having Data and application Migration as their work milestone <3 Projects - 5 Marks 3-5 Projects- 7 Marks >5 Projects- 10 Marks	10	Work orders or completion certificates from government/PSU projects Detailed case studies highlighting similar cloud projects, along with client references
6	URL for publicly mentioned price per month	To be annexed as part of technical proposal as per the format given in table below	-	Mandatory document to be eligible for Technical Presentation
7	Technical Presentation	Demonstration of Bidder's understanding of the project requirement- 5 Marks Plan for implementation/ Risk mitigation and adherence to SLA- 5 Marks Migration and Backup Strategy- 5 Marks High Availability and Security Plan- 5 Marks Challenges likely to be encountered and solution proposed- 5 Marks Work Plan, Team deployment and Adherence to Timelines- 5 Marks	30	Technical Presentation
Total			**100**	

Table for URL for publicly mentioned price per month

S. No.	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	URL for Column I
A	B	C	D	E	F	G	H	I	J
				vCPU	RAM (GB)				
1	Web Server	App	Ubuntu/Linux OS (Non-Burstable latest Generation AMD/Intel processors, Production Grade only)	8	32	2	Per VM per month		
2	Web Server	App	As above	16	64	2	Per VM per month		
3	Web Server	App	As above	4	16	1	Per VM per month		
4	Web Server	App	As above	8	64	4	Per VM per month		
5	Web Server	App	As above	16	128	1	Per VM per month		
6	Database	DB	CSP Managed MySQL as a service: 24*7 should vertically scale compute based on the workload demand and allow per second billing - Should support horizontal scaling by adding/removing read replicas - Should have ability to create OnDemand/manual backup/snapshots - Should support automatic backup from Standby to avoid IO activities suspension on primary node -Should support data caching	8	32	2	Per Instance per Month		
7	Database	DB	CSP Managed MySQL as a service: 24*7	16	64	2	Per Instanc		

S. No.	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	URL for Column I
A	B	C	D	E	F	G	H	I	J
			should vertically scale compute based on the workload demand and allow per second billing - Should support horizontal scaling by adding/removing read replicas - Should have ability to create OnDemand/manual backup/snapshots - Should support automatic backup from Standby to avoid IO activities suspension on primary node -Should support data caching				e per Month		
8	Storage	Managed Object Storage	Hot storage for frequent access	10			TB per Month		
9	Storage	Managed Object Storage	Cold storage for infrequent access	10			TB per Month		
10	Storage	Managed Blocked Storage	Single Disk with data redundancy 1024 GB SSD 20000 Sustained IOPS, 125 MB/Sec Sustained Throughput	4			Per disk per month		
11	Storage	Managed Blocked Storage	Single Disk with data redundancy 512 GB SSD 500 Sustained IOPS, 50 MB/Sec Sustained Throughput	10			Per disk per month		
12	Storage	Managed Blocked Storage	Single Disk 500 GB Storage and with data redundancy, Scalable IOPS and throughput to cater the requirement	10			Per disk per month		

S. No.	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	URL for Column I
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
13	Network and Security	Network Firewall	Stateful, support High Availability & SIEM Integration and logging	2			Unit per month		
14	Network and Security	VA Tool	Automated and Managed VA tool	10			Unit per month		
15	Key Management	HSM protection and Key operations	Keys	100			Per 100 Keys		
16	Key Management	HSM protection and Key operations	Keys operations	1000			Per 1000 Operations		
17	Log Monitoring	Log Analysis	Log Analysis and Monitoring	10GB			Unit per month		
18	Log Monitoring	Log Analysis	SIEM Services	1			Unit per month		
19	Backup	Managed backup tool	Managed backup tool	1			Unit per month		
20	VPN	Point to Point, Site to Site	Point to Point, Site to Site	10 Site to Site VPN connections 100 Client to Site VPN			Unit per month		
21	Load Balancer	Network and Traffic Load balancer	Network and Traffic Load balancer	1			Unit per month		
22	SSL		with encryption keys	10			Unit per year		
23	DNS Management	Network	Mapping of Domains	1			Per DNS per month		
24	Static Public IP	Network		1			Per IP Per month		
25	Data Transfer (Out)	Network		1 TB			Per GB per month		
26	Web Applica	Security	All traffic to the application to be	1			Unit per month		

S. No.	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	URL for Column I
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
	tion Firewall		routed through this WAF						
27	DDoS	Security		1			Unit per month		
28	IAM			10			Unit per month		
29	Antivirus			as per required VM			Per VM per month		

5.4 Evaluation Process:

a) General Instructions:

i. The evaluation of the responses to the Application will be done by an Evaluation committee of DBN.

ii. DBN may seek additional information and clarifications from any or all of the Bidders on the Pre-Qualification and Technical Responses submitted by the Bidder.

iii. The evaluation shall be strictly based on the information and supporting documents provided by the Bidders in the application submitted by them. It is the responsibility of the Bidders to provide all supporting documents necessary to fulfil the mandatory eligibility criteria. In case, information required by MeitY is not provided by Bidder, DBN may choose to proceed with evaluation based on information provided and shall not request the Bidder for further information. Hence, responsibility for providing information as required in this form lies solely with Bidder.

iv. The Evaluation Committee shall first evaluate the Pre-Qualification Response as per the Pre-Qualification Criteria above. The Pre-Qualification Response shall be evaluated based on the information provided in the **Section 5** and the supporting documents submitted.

v. The technical response of only those Bidders who qualify in the evaluation of the pre-qualification stage shall be opened.

vi. Each of the responses will be evaluated for compliance against the mandatory requirements in this Application Document. Only those Bidders who meet all the mandatory criteria and are found to be compliant against the requirements in this Application Document will be audited by STQC.

vii. Bidders are advised to exercise adequate care in quoting the prices. No modification/correction in quotations will be entertained once the bids/proposals are submitted. Even before submission of the proposal, care should be taken to ensure that any corrections/overwriting in the proposal are initialled by the person signing the proposal form.

viii. In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall be considered final.

ix. The results of the evaluation will be communicated to all the Bidders.

b) Scoring evaluation Process:

- **Evaluation of Pre-qualification Proposal:**

An "Evaluation Committee" would perform an initial review of the pre-qualification proposals and they shall be scrutinized for the responsiveness as set in the pre-qualification criteria, and for the completeness of required supporting documents as required to establish the Eligibility Claim.

- **Evaluation of Technical Proposal:**

Technical Evaluation of only eligible bidders would be carried out in the following manner:

a) The bidder's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and bidder is required to provide details on the proposed solution.

b) **Proposal Presentations**: The Committee shall invite each bidder to make a presentation to the DBN at a date, time and locations determined by the DBN. The purpose of such presentations would be to allow the bidders to present their understanding of scope of work, proposed solution, approach & methodology, implementation timelines, delivery readiness etc.to the committee.

c) The Evaluation Committee may undertake written clarifications from the bidders. The primary function of clarification in the evaluation process is to clarify ambiguities and uncertainties, if any, arising out of the evaluation of the bid documents.

d) Upon technical evaluation of each bid out of a maximum of 100 marks will be assigned to every bid.

e) The bidders who score **70 or more marks** in technical bid, will qualify for the evaluation of the financial bid.

f) The bidder with the highest marks in technical bid will be awarded 100 "**Technical Score**" and subsequently others bidders will also be awarded "**Technical Score**" relative to the highest technical marks for the final composite score calculation purpose e.g. if the highest technical marks is 90 then "**Technical Score**" is (90/90) × 100 = 100, hence the bidder with highest technical marks will score 100 "Technical Score". Similarly, another bidder who scored 80 marks, will get (80/90) x 100 = 88.88 "**Technical Score**". Following formula will be used for the "**Technical Score**" (TS) calculation:

$$\boldsymbol{Technical\ Score\ (TS) = \frac{(Bidder's\ Technical\ Marks\ (BTM))}{(Highest\ Technical\ Marks\ (HTM))} \times 100}$$

Stage-2 Evaluation of Financial Proposal

The evaluation will be carried out if financial bids are complete and computationally correct. The lowest financial bid will be awarded "**Financial Score**" of 100. The "**Financial Score**" of other bidder(s) will be computed by measuring the financial bids against the lowest financial bid. Following formula will be used for calculating "**Financial Score**":

$$\boldsymbol{Financial\ Score\ (FS) = \frac{(Lowest\ Financial\ Bid\ (LFB))}{(Bidder's\ Financial\ Bid\ (BFB))} \times 100}$$

Stage-3 Computation of Composite Bid Score

The "**Composite Bid Score**" is a weighted average of the Technical and Financial Scores. The ratio of Technical and Financial Scores is 70:30 respectively. The Composite Bid Score will be derived using the following formula:

Composite Bid Score = ((TS × 0.70) + (FS × 0.30))

The responsive bidder(s) will be ranked in descending order according to the Composite Bid Score, which is calculated based on the above formula. The highest-ranking bidder as per the Composite Bid Score will be selected for award of contract.

6 Service Level Agreements:

Following table depicts the service levels that bidder needs to be adhere to:

No.	KPI Description	Measurement Criteria	Penalty
1	Availability (Cloud, Network and Security components/services)	Shall be measured using below formula: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month)/Total No. of Hours in the calendar month] x100}	a) Baseline: 99.5 % Uptime for every single service. b) Uptime <99.5 % & >= 99 will attract a penalty of 2% of the quarterly billing. c) Uptime <99% & >= 98% will attract a penalty of 5 % of the quarterly billing. d) Anything below 98% will attract 5% penalty for every 1 percent drop in uptime and may lead to

No.	KPI Description	Measurement Criteria	Penalty
			the termination of contract.
2	Availability of regular reports (SLA, Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Baseline- Reports shall be submitted within 5 days **Penalty**- a) = 6 working days - 1% of Quarterly Payment for the Project b) = 11 working days - 2% of Quarterly Payment for the Project c) For the delay beyond 15 days, penalty of 3% of the Quarterly Payment for the Project
3	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 2% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 3% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 5% of Quarterly Payment of the Project. d) <98% - 8% of the Quarterly Payment of the Project In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 10% of the Quarterly Payment of the Project.
4	Provisioning of new Virtual Machine and/or container and/or other services (GPU, Storage, Managed DBs etc.)	Time to provision new Virtual Machine Measurement shall be done by analysing the log files	**Baseline-** 95% Within 5 minutes **Penalty-** i. <95% to =>90% - 1% of quarterly payment of the service ii. <90% to =>85%- 3% of quarterly payment of the service Iii. <85% to =>80% - 5% of the quarterly payment of the service iv. <80%- 10% of the quarterly payment of the service

No.	KPI Description	Measurement Criteria	Penalty
5	Spinning up the Object and Block Storage	Time to spin up Object Storage Measurement shall be done by analysing the log files and Time to spin up to 100 GB Block Storage and attach it to the running VM Measurement shall be done by analysing the log files	**Baseline-** 98% Within 15 minutes **Penalty-** i. <95% to =>90% - 1% of quarterly payment of the service ii. <90% to =>85%- 3% of quarterly payment of the service Iii. <85% to =>80% - 5% of the quarterly payment of the service iv. <80%- 10% of the quarterly payment of the service
6	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analysing the log files and Cloud Service (API) reports.	**Baseline-** Within 15 minutes **Penalty**- i. Within 15 minutes no penalty ii. More than 15 Minute - 1% of the Quarterly Payment of that Service
7	Response Time under Basic Support	Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month	**Baseline-** 95% Within 60 minutes **Penalty-** i. <95% to =>90% - 2% of quarterly payment of the service ii. <90% to =>85%- 3% of quarterly payment of the service Iii. <85% to =>80% - 5% of the quarterly payment of the service iv. <80%-7% of the quarterly payment of the service
8	Data Migration	Migration of data from the source to destination system	**Baseline**-Error rate to be <0.25% **Penalty**

No.	KPI Description	Measurement Criteria	Penalty
			-a) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the Project b) Error Rate > 0.30% & <=0.35% - 2% of the Quarterly Payment of the Project c) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the Project. For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Payment of the Project will be levied as additional liquidity damage
9	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)	For each breach/data theft, penalty will be levied as per following criteria. 1. Severity 1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity 2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity 3 (as define in Annexure A) - Penalty of Rs 5 Lakh per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << Government Department / Agency>> reserves the right to terminate the contract.
10	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017:2015, ISO27018:2019, ISO20001:2018 etc.)	**Baseline-** All certificates should be valid during the Project duration **Penalty-** Delay in sustenance of certifications a) > 1 day & <= 5 days - 1% of the Quarterly Payment of the Project b) > 5 day & <= 15 days - 2% of the Quarterly Payment of the Project

No.	KPI Description	Measurement Criteria	Penalty
		should lapse within the Project duration. Service Provider should ensure the sustenance/renewal of the certificates	c) > 15 day & <= 30 days - 3% of the Quarterly Payment of the Project d) > 30 days, 5% of the Quarterly Payment of the Project
11	Non-closure of audit observations	No observation to be repeated in the next audit. To be checked in next audit report	**Baseline-** All audit observations to be closed within defined timelines **Penalty**- for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 1% of the Quarterly Payment of the Project b) > 10 % & <= 20% - 2% of the Quarterly Payment of the Project c) > 20 % & <= 30% - 4% of the Quarterly Payment of the Project d) >30% - 10% of the Quarterly Payment of the Project
12	Security log monitoring (includes infrastructure assets) and Event Notification	Reporting of security incidents/threats. 24x7 monitoring of all in-scope Infra	**Baseline:** Detecting and reporting within 15 minutes >15 minutes & <= 30 minutes will attract a penalty of 2% of the O&M (Operations and Maintenance) quarterly billing. >30 minutes & <= 1 hour will attract a penalty of 3% of the O&M (Operations and Maintenance) quarterly billing. For each additional hour after 1 hours, liquidated damages of 0.5% will be levied as additional liquidated damages
13	Availability of all manpower resources as proposed	Actual number of man-days deployed)/ (Actual	**Baseline-** On the Day of Award of work (T) 50% of Manpower are available

No.	KPI Description	Measurement Criteria	Penalty
		number of man-days per month)	**Penalty-** 1% of Quarterly Payment of the service
			Baseline- On T+30 Days, 75% of Manpower available. **Penalty-** 3% of Quarterly Payment of the service.
			Baseline- T+60 Days 100% of Manpower available. **Penalty**- 5% of Quarterly Payment of the service
14	Replacement of the resources	Replacement of manpower resources after the Go-Live the period	**Baseline-** Within 7 Days equivalent or better candidate **Penalty-** Rs 10,000/Day until the replaced candidates join
15	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analysing security audit reports	**Baseline-**95% within 8 Hrs. of the notification **Penalty as indicated below (per occurrence):** a) = 90.00% - 2% of Quarterly Payment of the Project b) = 85.0% - 4% of Quarterly Payment of the Project c) = 80.0% - 7% of Quarterly Payment of the Project d) <80% - 10% of the Quarterly Payment of that Project

No.	KPI Description	Measurement Criteria	Penalty
16	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage-based threshold Measurement shall be done by analysing the log files	**Baseline-** 99% within 10 mins of crossing the Threshold Penalty as indicated below (per occurrence): a) = 95.00% - 0.25% of Quarterly Payment of the Project b) = 90.0% - 0.5% of Quarterly Payment of the Project c) = 85.0% - 0.75% of Quarterly Payment of the Project d) <85% - 1% of the Quarterly Payment of that Project

7 Severity Levels:

Severity Level	Description	Examples
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	Non-availability of VM. No access to Storage, software or application
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

8 Project Activity and Timelines:

Sr. No.	Activity	Timelines	Payment	Deliverables
1	Contract Signing and Award of Contract	**T+0 Days**	Nil	Signed Work Order
2	Project Plan and As-Is Assessment team deployment	**T+7 Days**	Nil	Project Plan Document and CV of team deployed
3	As-Is Assessment	**T+15 Days**	Nil	Assessment report
4	Cloud Provisioning	**T+20 Days**	Nil	Report on the deployment along with the details of the resources and credentials of provisioned cloud
5	Application and Data Migration	**T+30 Days**	50% payment after 30 days of application & data migration and balance 50% payment after 60 days of application & data migration	Acceptance letter from DBN for successful Migration
6	Operational Cost	Recurring, Quarterly **T+730** Days	As per actuals	Signed MPR with details of activity performed during the month
7	Cloud Cost	Recurring, Quarterly **T+730 Days**	As per actuals	Actual cloud usage bill along with utilization reports

9 Payment Terms:

i. All the payments are subject to satisfactory work completion/Milestone completion certificate obtained from the DBN.
ii. Cloud Infra and other recurring cost shall be calculated after considering SLAs mentioned in this RFP Document.
iii. Payment shall be made within 45 Days of receiving the invoice from the selected bidder along with satisfactory work completion certificate for the billed period.

Annexure A: Technical Bid Submission Form

[Location, Date]
To
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka road, Sanchar Bhawan, New Delhi – 110001

RFP dated [date] for selection of the Bidder for [name of assignment]

Dear Sir/Madam,

With reference to your RFP Document [GeM No] dated [date], we, having examined all relevant documents and understood their contents, hereby submit our Technical Bid Proposal for selection as [name of assignment]. The Proposal is unconditional.

We are submitting our Proposal as [name of the Bidder.]

We understand you are not bound to accept any Proposal you receive.
Further:

1. We acknowledge that DBN will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Bidder, and we certify that all information provided in the Proposal and in the supporting documents is true and correct, nothing has been omitted which renders such information misleading; and all documents accompanying such Proposal are true copies of their respective originals.
2. This statement is made for the express purpose of appointment as the Selected Agency for the aforesaid Project.
3. We shall make available to DBN any additional information it may deem necessary or require for supplementing or authenticating the Proposal.
4. We acknowledge the right of DBN to reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any account whatsoever.
5. We certify that, we have neither failed to perform on any assignment or contract, as evidenced by imposition of a penalty by an arbitral or judicial authority or a judicial pronouncement or arbitration award against the Bidder, nor been expelled from any project, assignment or contract by any public authority nor have had any assignment or contract terminated by any public authority for breach on our part.
6. We declare that:
    a. We have examined and have no reservations to the RFP, including any Addendum issued by DBN
    b. We do not have any conflict of interest in accordance with the terms of the RFP.

c. We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as defined in the RFP document, in respect of any tender or request for proposal issued by or any agreement entered into with DBN or any other public sector enterprise or any government, Central or State; and

d. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice.

7. We understand that you may cancel the selection process at any time and that you are neither bound to accept any Proposal that you may receive nor to select the Bidder, without incurring any liability to the other Bidder.
8. We certify that in regard to matters other than security and integrity of the country, we or any of our affiliates have not been convicted by a court of law or indicted or adverse orders passed by a regulatory authority which would cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.
9. We further certify that in regard to matters relating to security and integrity of the country, we have not been charge-sheeted by any Agency of the Government or convicted by a court of law for any offence committed by us or by any of our affiliates. We further certify that neither we nor any of our consortium members have been barred by the central government, any state government, a statutory body or any public sector undertaking, as the case may be, from participating in any project or bid, and that any such bar, if any, does not subsist as on the date of this RFP.
10. We further certify that no investigation by a regulatory authority is pending either against us or against our affiliates or against our CEO or any of our Directors/ Managers/ employees.
11. We hereby irrevocably waive any right or remedy which we may have at any stage at law or howsoever otherwise arising to challenge or question any decision taken by DBN in connection with the selection of the Bidder or in connection with the selection process itself in respect of the above-mentioned Project.
12. We agree and understand that the proposal is subject to the provisions of the RFP document. In no case, shall we have any claim or right of whatsoever nature if the Project is not awarded to us or our proposal is not opened or rejected.
13. We agree to keep this offer valid for 180 (one eighty) days from the Proposal Due Date specified in the RFP. Further, we also agree to extend the validity of bid for such further period as may be requested by DBN.
14. A Power of Attorney in favour of the authorized signatory to sign and submit this Proposal and documents are attached herewith.
15. The Technical and Financial Proposal is being submitted in a separate cover. This Pre-Qualification Proposal read with the Technical and Financial Proposal shall constitute the application which shall be binding on us.
16. We agree and undertake to abide by all the terms and conditions of the RFP Document.

Yours sincerely,

(Signature)

Name and title of Authorized
Signatory/Authorized representative
(Name of Firm)
Address:
Telephone:
(Name and seal of the Bidder/Member in Charge)

Annexure B: Self-certification of not being blacklisted

[On the letterhead of the organisation]

[Location, Date]

In response to the RFP No. Dated , Proposal Invited for the Selection of the [Insert title of assignment] I/ We hereby declare that presently our Company/ firm _ _ _ __ _ _ _ _ _ _ _ _ _ _ _ _ _ _ is having unblemished record and is not declared ineligible for corrupt & fraudulent practices in similar services either indefinitely or for a particular period of time by any State/ Central Government/ PSU/Autonomous Body during last three years preceding the date of submission of bid.

We further declare that presently our Company/ firm _____is not debarred and not declared ineligible for reasons other than corrupt & fraudulent practices in similar services by any State/ Central Government/ PSU/ Autonomous Body on the date of Bid Submission during last three years preceding the date of submission of bid.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Yours faithfully,

Name of the Bidder: -
Authorized Signatory: -
Seal of the Organization: -
Date:
Place:

Annexure C: Format for highlighting experience

Assignment name:	**Approx. value of the contract (in INR):**
Country: **Location within country:**	**Duration of assignment (Months):**
Name of Organisation:	**Total No of staff-months of the assignment:**
Address:	**Approx. value of the services provided by your** **firm under the contract:**
Start date (month/year): **Completion date (month/year):**	**No of professional staff-months provided by** **associated Consultants:**
Status of the project (completed/partially completed/on-going etc.):	**Two references of the Organisation (Name,** **Designation & Contact details along with email-** **id)**
Name of senior professional staff of your firm **involved and functions performed (indicate most significant profiles such as Project Director/ Project Lead etc.):**	**Name of associated Consultants, if any:**
Narrative description of Project:	
Description of actual services provided by your staff within the assignment:	

- *Kindly provide supporting documents such as contract/work order copy LOI/completion certificate etc.*
- *Please note that the experience will not be counted if the relevant supporting document is not attached.*
- *Please attach a clear scan copy of the supporting documents*

Annexure D: Format for Power of Attorney for Authorized Representative

Know all men by these presents, We, [name of organization and address of the registered office] do hereby constitute, nominate, appoint and authorize Mr. / Ms. [name], son/ daughter/ wife of [name], and presently residing at [address], who is presently employed with/ retained by us and holding the position of [designation] as our true and lawful attorney (hereinafter referred to as the —Authorized Representative), with power to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our Proposal for and selection as Selected Agency for [name of assignment], to be developed by Bidder including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-bid and other conferences and providing information/ responses to DBN, representing us in all matters before DBN and undertakings consequent to acceptance of our proposal and generally dealing with DBN in all matters in connection with or relating to or arising out of our Proposal for the said Project and/or upon award thereof to us until accepting the work order with DBN.

AND we do hereby agree to ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Authorized Representative pursuant to and in exercise of the powers conferred herein and that all acts, deeds and things done by our said Authorized Representative in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, [name of organization], THE ABOVE-NAMED PRINCIPAL HAVE EXECUTED

THIS POWER OF ATTORNEY ON THIS [date in words] DAY OF [month] [year in YYYY format].

For [name and registered address of organization]
[Signature]
[Name]

[Designation]
Witnesses:

1. [Signature, name, and address of witness]
2. [Signature, name, and address of Authorized Representative] Accepted

Annexure E: Format for Bid Securing Declaration

On the letterhead of the organisation]

[Location, Date]

To:
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka Road, Sanchar Bhawan, New Delhi – 110001

Ref: RFP Document No. RFP No.: 30-40/2022/USOF/PMU/Part-II; Tender Title: Selection of Managed Service Provider for Migration, Hosting & Operations of IT applications of Digital Bharat Nidhi on MeitY empanelled Cloud

Sir/ Madam

We, the undersigned, solemnly declare that:

We understand that according to this RFP document's conditions, the Proposal must be supported by a Bid Securing Declaration In lieu of Bid Security.

We unconditionally accept the conditions of this Bid Securing Declaration. We understand we shall stand automatically suspended from being eligible for bidding in any tender in Procuring Organisation (DBN) for 2 years from the date of opening of this Proposal if we breach our obligation(s) under the tender conditions if we:

1) Withdraw/ amend/ impair/ derogate, in any respect, from our Proposal, within the Proposal validity; or
2) Being notified within the Proposal validity of the acceptance of our Proposal by the DBN:
   (a) Refused or failed to produce the original documents for scrutiny or the required Performance Security within the stipulated time under the RFP conditions.
   (b) Fail or refuse to sign the contract.

We know that this Proposal-Securing Declaration shall expire

1) If the contract is not decided - forty-five days after the expiration of the Proposal validity, any extension to it.
2) If the contract is not awarded to us - not later than thirty days after the conclusion of the resultant contract, or
3) If the contract is awarded to us - after receipt of performance security from them

For [name and registered address of organization]
[Signature]
[Name]
[Designation]

Annexure F: Format for Bank Guarantee for Earnest Money Deposit

BG No.

Date:

1. In consideration of you, Digital Bharat Nidhi, Department of Telecommunications, Ministry of Communications, Government of India, Sanchar Bhawan, New Delhi — 110001 (hereinafter referred to as the Authority which expression shall, unless repugnant to the context or meaning thereof, include its administrators, successors and assigns) having agreed to receive the proposal of [Name of company], (hereinafter referred to as the —Bidder which expression shall unless it be repugnant to the subject or context thereof include its successors and assigns), for appointment as Selected Agency for [name of assignment] pursuant to the RFP Document dated [date] issued in respect of the Assignment and other related documents including without limitation the draft work order for services (hereinafter collectively referred to as —RFP Documents), we [Name of the Bank] having our registered office at [registered address] and one of its branches at [branch address] (hereinafter referred to as the —Bank), at the request of the Bidder, do hereby in terms of relevant clause of the RFP Document, irrevocably, unconditionally and without reservation guarantee the due and faithful fulfilment and compliance of the terms and conditions of the RFP Document by the said Bidder and unconditionally and irrevocably undertake to pay forthwith to DBN an amount of Rs. [in figures] ([in words]) (hereinafter referred to as the —Guarantee) as our primary obligation without any demur, reservation, recourse, contest or protest and without reference to the Bidder if the Bidder shall fail to fulfil or comply with all or any of the terms and conditions contained in the said RFP Document.

2. Any such written demand made by DBN stating that the Bidder is in default of the due and faithful fulfilment and compliance with the terms and conditions contained in the RFP Document shall be final, conclusive, and binding on the Bank. We, the Bank, further agree that DBN shall be the sole judge to decide as to whether the Bidder is in default of due and faithful fulfilment and compliance with the terms and conditions contained in the RFP Document including, Document including without limitation, failure of the said Bidder to keep its Proposal valid during the validity period of the Proposal as set forth in the said RFP Document, and the decision of DBN that the Bidder is in default as aforesaid shall be final and binding on us, notwithstanding any differences between DBN and the Bidder or any dispute pending before any court, tribunal, arbitrator or any other authority.

3. We, the Bank, do hereby unconditionally undertake to pay the amounts due and payable under this Guarantee without any demur, reservation, recourse, contest or protest and without any reference to the Bidder or any other person and irrespective of whether the claim of DBN is disputed by the Bidder or not, merely on the first demand from DBN stating that the amount claimed is due to DBN by reason of failure of the Bidder to fulfil and comply with the terms and conditions contained in the RFP Document including without limitation, failure of the said Bidder to keep its Proposal valid during the validity period of the Proposal as set forth in the said RFP Document for any reason whatsoever. Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this Guarantee. However, our liability under this Guarantee shall be restricted to an amount not exceeding Rs. [in figures] ([in words]).

4. This Guarantee shall be irrevocable and remain in full force for a period of 60(sixty) days from the Proposal Due Date and a further claim period of 30 (thirty) days or for such extended period as may be mutually agreed between DBN and the Bidder, and agreed to by the Bank, and shall continue to be enforceable until all amounts under this Guarantee have been paid.
5. The Guarantee shall not be affected by any change in the constitution or winding up of the Bidder or the Bank or any absorption, merger or amalgamation of the Bidder or the Bank with any other person.
6. To give full effect to this Guarantee, DBN shall be entitled to treat the Bank as the principal debtor. DBN shall have the fullest liberty without affecting in any way the liability of the Bank under this Guarantee from time to time to vary any of the terms and conditions contained in the said RFP Document or to extend time for submission of the Proposals or the Proposal validity period or the period for conveying of Letter of Acceptance to the Bidder or the period for fulfilment and compliance with all or any of the terms and conditions contained in the said RFP Document by the said Bidder or to postpone for any time and from time to time any of the powers exercisable by it against the said Bidder and either to enforce or forbear from enforcing any of the terms and conditions contained in the said RFP Document or the securities available to DBN, and the Bank shall not be released from its liability under these presents by any exercise by DBN of the liberty with reference to the matters aforesaid or by reason of time being given to the said Bidder or any other forbearance, act or omission on the part of DBN or any indulgence by DBN to the said Bidder or by any change in the constitution of DBN or its absorption, merger or amalgamation with any other person or any other matter or thing whatsoever which under the law relating to sureties would but for this provision have the effect of releasing the Bank from its such liability.
7. Any notice by way of request, demand or otherwise hereunder shall be sufficiently given or made if addressed to [Name of bank along with branch address] and sent by courier or by registered mail to the Bank at the address set forth herein.
8. We undertake to make the payment on receipt of your notice of claim on us addressed to [Name of bank along with branch address] and delivered at our above branch which shall be deemed to have been duly authorized to receive the said notice of claim.
9. It shall not be necessary for DBN to proceed against the said Bidder before proceeding against the Bank and the guarantee herein contained shall be enforceable against the Bank, notwithstanding any other security which DBN may have obtained from the said Bidder or any other person and which shall, at the time when proceedings are taken against the Bank hereunder, be outstanding or unrealized.
10. We, the Bank, further undertake not to revoke this Guarantee during its currency except with the previous express consent of DBN in writing.
11. The Bank declares that it has power to issue this Guarantee and discharge the obligations contemplated herein, the undersigned is duly authorized and has full power to execute this Guarantee for and on behalf of the Bank.
12. For the avoidance of doubt, the Bank's liability under this Guarantee shall be restricted to Rs. [in figures] ([in words]).

The Bank shall be liable to pay the said amount or any part thereof only if DBN serves a written claim on the Bank in accordance with paragraph 8 hereof, on or before [date].

Signed and delivered by [name of bank]
By the hand of Mr. /Ms. [name], it's [designation] and authorized official.
(Signature of the Authorized Signatory)

(Official Seal)

Notes:
1. The Bank Guarantee should contain the name, designation and code number of the officer(s) signing the Guarantee.
2. The address, telephone number and other details of the Head Office of the Bank as well as of issuing Branch should be mentioned on the covering letter of issuing Branch.

Annexure G: Format for Technical Proposal Submission Form

[Location, Date]
To:
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka Road, Sanchar Bhawan, New Delhi – 110001

Dear Sir
We, the undersigned, offer to provide the services for [Insert title of assignment] in accordance with your Request for Proposal dated [Insert Date] and our Proposal. We are hereby submitting our Proposal, which includes a Technical Proposal, and a Financial Proposal.

We hereby declare that all the information and statements made in this Proposal are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Proposal is accepted, to initiate the work related to the assignment at a date mutually agreed between us.

We understand you are not bound to accept any Proposal you receive.

We remain,
Yours sincerely,
Authorized Signature [In full and initials]: _____
Name and Title of Signatory: _____
Name of Firm: _____
Address: _____

Annexure H: Format for Bidder Profile

- Name of organization
- Nature of the legal status in India
- Legal status reference details
- Nature of business in India
- Date of Incorporation
- Date of Commencement of Business
- Address of the Headquarters
- Address of the Registered Office in India
- Address of the Data Center Facility
- Other Relevant Information

Mandatory Supporting Documents:
- Certificate of Incorporation from Registrar of Companies (ROC)

Annexure I: Financial Details of the Organization

Financial details of the organization as per the format below. Enclose the mandatory supporting documents listed in format.

Financial Information of <<Bidder / Holding Company>> (The CSP can cite only single unique holding company and not multiple ones)			
	FY 2021-22	**FY 2022-23**	**FY 2023-24**
Net Worth (in INR Crores)			
Revenue from the Cloud / Data Centre Hosting services or both (in INR Crores)			
Other Relevant Information			

Mandatory Supporting Documents:
- Auditor Certificate for the last three financial years: FY 2020-21, FY 2021-22 and FY 2022-23 indicating the Net Worth and Revenue from the Cloud /Data Centre hosting services or both

Annexure J: Compliance Requirements

CSPs are required to show their compliances to the requirements specified in

Section 3 Technical Compliance Document.

Annexure K: Details of the Data Centre Facility and Cloud Service Offerings in India

(IN CASE THE BIDDER CHOOSES TO OFFER THE CLOUD SERVICES PROPOSED FOR EMPANELMENT FROM MULTIPLE DATA CENTER FACILITIES, PLEASE PROVIDE THE DETAILS OF EACH OF THE DATA CENTER FACILITIES IN THE FORMAT BELOW)

Details of the Data Center Facility	
Address of the Data Centre Facility	<<street and mailing addresses, phone, fax and email>>
Month / Year of Starting the Data Centre Operations	Month & Year
Operational Capacity (Number of Racks)	<<Number >>
Availability of Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centers, Backup, Operations Management, and Data Management	<<Yes / No>>
Security Features available including Physical Security (Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting))	<<Yes / No>>
Tier Level and certifications (Conformance to at least Tier III standard, preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party)	<<Yes / No>> In case certified, details of the Certification
Certified for ISO 27001:2017	<<Yes / No>> Details of the Certification
NOC offered for the Data Centre and the managed services quality should be certified for ISO 20000-1:2018	<<Yes / No>> Details of the Certification
Other Relevant Information	
Mandatory Supporting Documents:	

a) ISO 27001 (year 2017) Certification b) ISO 20000-1:2018 Certification Details c) TIA 942 or UPTIME Certification d) ISO 27017 (2015) Certification e) ISO 27018 (2019) Certification

Annexure L: Format to Attend the pre-bid Meeting

Name of the Company/Firm:
Address of the Company/Firm:
Name of Person(s) Representing the Company/ Firm:

Name of the Person	Designation	E-mail ID	Contact No

Sl. No.	Application document reference(s) (section number/ page)	Content of Application document requiring clarification	Points on which clarification required

Annexure M: Format of Performance of Bank Guarantee PBG

To,
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka Road, Sanchar Bhawan, New Delhi – 110001

Sub: Performance Guarantee for _____

Dear Sir,
This Deed of Guarantee executed by the _____ (Bank name) a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and carrying out banking business including guarantee business and having its head office at……..(hereinafter referred to as "the Bank") in favour of Digital Bharat Nidhi, Department of Telecommunication, Government of India and having its registered office at 20, Ashoka Rd, Sansad Marg Area, New Delhi, Delhi 110001 for Development of _____ (name(s) _____ (Rupees _____) (Approx.___% of _____), being the total value of the items purchased including all taxes) after supply and installation of the items towards performance warrantee of the item (s) Supplied.

This Guarantee is issued subject to the condition that the liability of the bank under \ this guarantee is limited to a maximum of _____ (Rupees_____ only) and the Guarantee Shall remain in force up to (_____) year from the date of Issue of this Bank Guarantee and cannot be invoked, otherwise than by a written demand or claim under this guarantee served on the Bank on or before _____ by Department of Telecom, New Delhi. And whereas the bank_____ (name and address) has agreed to give on behalf of the Supplier a Guarantee.
Therefore, we hereby affirm that we unconditionally Guarantee and are responsible to you on behalf of the Supplier, up to a total amount of
_____(Rupees_____only) and we undertake to pay you, at the very first instance without any demur upon your demand without cavil or argument, any sum or sums as specified by you within or up to the limit of _____(Rupees_____) i.e. the amount of bank guarantee as aforesaid, without your need to prove or to show grounds or reasons for your demand of the sum specified therein. This Guarantee shall not be affected by any change in the Constitution of the Bank or supplier or beneficiary.
NOTWITHSTANDING ANYTHING CONTAINED HEREIN

The bank hereby covenants and declares that the guarantee hereby given is an irrevocable on and shall not be revoked under any circumstances and/ or by a Notice or otherwise.
The Bank agrees that the amount hereby guaranteed shall be due and payable to DBN on serving us with a notice before expiry of Bank Guarantee requires the payment of the amount and such

notice shall be deemed to have been served on the bank either by actual delivery thereof to the Bank or by registered post at the address of the Bank.

This guarantee shall remain in force up to_____ provided that if so desired by DBN, this guarantee shall be renewed at the instance of supplier or DBN for a further period as may be indicated by them on the same terms and conditions as contained therein.

Dated at This Day of

SEALED & SIGNED BY THE BANK

Note: for information

1. The guarantee should be furnished by a Nationalized Bank/Scheduled Bank, authorized by RBI to issue a Bank Guarantee.
2. This bank guarantee should be furnished on stamp paper specified for the purpose.
3. The stamp paper should have been purchased in the Name of the Bank executing the Guarantee.
4. The PBG must be routed through Structured Financial Messaging System (SFMS) from issuing bank to DBN bank as given in the tender document by sending IFN 760 COV Bank Guarantee Advice Message. Thereafter only physical Bank Guarantee shall be taken as submitted and become operational.

Annexure N: Format of Financial Proposal Submission Form

[On the letterhead of the organisation]

[Location]
[Date]

To
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka Road, Sanchar Bhawan, New Delhi-110001

Dear Sir/ Madam,

Subject: RFP for [name of assignment].

We, the undersigned, offer to provide the RFP for [name of assignment] in accordance with your Request for Proposal dated [date] and our Proposal. Our attached Financial Proposal is for the sum of [amount(s) in words and figures] (including GST)

Our Financial Proposal shall be binding upon us subject to the modifications resulting from arithmetic correction, if any, up to expiration of the validity period of the Proposal, i.e. [date].

We undertake that, in competing for (and, if the award is made to us, in executing) the above assignment, we will strictly observe the laws against fraud and corruption in force in India namely —Prevention of Corruption Act 1988.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Firm: Address:

Annexure O:

Table A-Format of Summary of Costs:

S. No.	Description	Schedule	Total Price (INR)
1	One Time Cost	Table B: Total	
2	Total OPEX Cost including Managed Services Cost as per Table C for Two Years	Table C: Total	
3	**Grand Total (Bid Value) = Table B + Table C**		

Note:
1. Prices shall be quoted in INR only as against the line items mentioned in Table B and Table C
2.All the prices excluding the Taxes and Taxes will be applicable as actuals
3. Payments shall be made to the selected bidder on a quarterly equated basis as per the actual consumption of resources as mentioned in Table C for the entire contract duration
4. The Bid Value shall be inclusive of all the installation, commissioning, testing and any other price that might be incurred by the Bidder for the performance of the contract
5. One Time Cost & OPEX ratio shall be reasonable and realistic, a bid shall not be considered for Final Evaluation if the total One Time Cost value happens to be more than 20% of the overall bid value
6. Line-Item Cost quoted by Bidder for the entire Bill of Material (BoM) shall be valid for the entire contract duration and if it is found that (in future) public pricing for mentioned resources is lower than cost mentioned in bid, lower cost shall be considered.
7. Bidder is mandatorily required to put cost/value against each of the Line Item; in absence of any value against the specific Line Item then the Cost for that specific line item shall be considered as Zero which shall be applicable for the entire contract duration
8. Bidder shall quote one time cost and managed services cost considering scope document of the RFP and any additional Tool/Software required to deliver the ask Scope then the respective Cost should include into, either one time cost or Managed services cost head.
9. DBN at its sole discretion may alter (increase/decrease) quantity or may remove item
10. DBN may procure any other item which is not in the BOQ considering the overall discount.
11. DBN is free to opt for any service or configuration of service in the host of offerings of the CSP.
12. Prices shall be over and above the free tier provided by Cloud Service Providers and billing shall be done as per actual usage.

Table B - One time Cost:

S. No.	Description	Total Price (INR) (excluding Taxes)
		A
1.	One-time cost of setting up cloud infrastructure and Setting up Managed Services environment for the period of Two (2) Years including helpdesk & SLA monitoring setup for provisioned cloud infrastructure	
2.	One-time cost for Migration Services for all existing Setup & applications on the Cloud	
Total		

Table C- OPEX Cost:

Sr. No	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	Offered price per month as per the mentioned quantity	Discount %
				vCPU	**RAM (GB)**					
1	Web Server	App	Ubuntu/Linux OS (Non-Burstable latest Generation AMD/Intel processors, Production Grade only)	8	32	2	Per VM per month			
2	Web Server	App	As above	16	64	2	Per VM per month			
3	Web Server	App	As above	4	16	1	Per VM per month			
4	Web Server	App	As above	8	64	4	Per VM per month			
5	Web Server	App	As above	16	128	1	Per VM per month			
6	Database	DB	CSP Managed MySQL as a service: 24*7 should vertically scale compute based on the workload demand and allow per second billing - Should support horizontal scaling by adding/removing read replicas - Should have ability to create OnDemand/manual backup/snapshots - Should support automatic backup from Standby to avoid IO activities suspension on primary node -Should support data caching	8	32	2	Per Instance per Month			

Sr. No	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	Offered price per month as per the mentioned quantity	Discount %
7	Database	DB	CSP Managed MySQL as a service: 24*7 should vertically scale compute based on the workload demand and allow per second billing - Should support horizontal scaling by adding/removing read replicas - Should have ability to create OnDemand/manual backup/snapshots - Should support automatic backup from Standby to avoid IO activities suspension on primary node -Should support data caching	16	64	2	Per Instance per Month			
8	Storage	Managed Object Storage	Hot storage for frequent access	10			TB per Month			
9	Storage	Managed Object Storage	Cold storage for infrequent access	10			TB per Month			
10	Storage	Managed Blocked Storage	Single Disk with data redundancy 1024 GB SSD 20000 Sustained IOPS, 125 MB/Sec Sustained Throughput	4			Per disk per month			
11	Storage	Managed Blocked Storage	Single Disk with data redundancy 512 GB SSD 500 Sustained IOPS, 50 MB/Sec Sustained Throughput	10			Per disk per month			
12	Storage	Managed Blocked Storage	Single Disk 500 GB Storage and with data redundancy,	10			Per disk per month			

Sr. No	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	Offered price per month as per the mentioned quantity	Discount %
			Scalable IOPS and throughput to cater the requirement							
13	Network and Security	Network Firewall	Stateful, support High Availability & SIEM Integration and logging	2			Unit per month			
14	Network and Security	VA Tool	Automated and Managed VA tool	10			Unit per month			
15	Key Management	HSM protection and Key operations	Keys	100			Per 100 Keys			
16	Key Management	HSM protection and Key operations	Keys operations	1000			Per 1000 Operations			
17	Log Monitoring	Log Analysis	Log Analysis and Monitoring	10GB			Unit per month			
18	Log Monitoring	Log Analysis	SIEM Services	1			Unit per month			
19	Backup	Managed backup tool	Managed backup tool	1			Unit per month			
20	VPN	Point to Point, Site to Site	Point to Point, Site to Site	10 Site to Site VPN connections 100 Client to Site VPN			Unit per month			
21	Load Balancer	Network and Traffic Load balancer	Network and Traffic Load balancer	1			Unit per month			
22	SSL		with encryption keys	10			Unit per year			
23	DNS Management	Network	Mapping of Domains	1			Per DNS per month			
24	Static Public IP	Network		1			Per IP Per month			

Sr. No	Type	Type of Service	Technical specs and requirements	Configuration		Quantity	Unit	Publicly mentioned price per month as per the mentioned quantity	Offered price per month as per the mentioned quantity	Discount %
25	Data Transfer (Out)	Network		1 TB			Per GB per month			
26	Web Application Firewall	Security	All traffic to the application to be routed through this WAF	1			Unit per month			
27	DDoS	Security		1			Unit per month			
28	IAM			10			Unit per month			
29	Antivirus			as per required VM			Per VM per month			
Weighted Average discount										

Note- Compute, Storage, Network and Security components mentioned in the list above and to be added by proposed MSP (if any) is to be self-configurable to cater to varies requirement of the DBN such as various traffic scenarios, IOPS, bandwidth etc.

Any other item not covered above shall be procured at the weighted average discount calculated as per the offered discount.

Annexure P: Undertaking on Absence of Conflict of Interest

[On the letterhead of the organisation]

[Location]
[Date]

To
Administrator, Digital Bharat Nidhi
Department of Telecommunications
Ministry of Communications, Government of India
Ashoka Road, Sanchar Bhawan, New Delhi-110001

Dear Sir/ Madam,

Ref: Undertaking on Absence of Conflict of Interest

I/We as Bidder do hereby undertake that there is absence of, actual or potential conflict of interest on the part of our organization or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with DBN. I/We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of our organization to comply with the requirements as given in the application document.

We undertake and agree to indemnify and hold DBN harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) by DBN and/or its representatives, if any such conflict arises later.

Yours sincerely,
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Firm:
Address:

Annexure Q: Details of Existing Applications

The above applications are hosted on 2 servers provided by NIC and the configuration of each server is 4vCPU, 16GB RAM and 1 TB Storage. These applications make use of both MySQL and Postgres database.

Annexure R: Manpower Details

The Bidder should furnish the project team details such as the qualifications, experience, certification, and other details as per format given below along with detailed CVs.

S. No	Role	Name of the Resource	Date Of Birth	Qualifications	Relevant Certifications	Total IT Experience (Years)	Experience in the Proposed Role (Years)	Compliance - Yes/No

Note: It is mandatory that the resource proposed for the Project Manager position should not change till Go-Live of the DBN Cloud Migration project.

Manpower/ Resource requirements:

S. No.	Role	Quantity
1.	**Project Manager (10+ Years of Exp)**	1
2.	Cloud and Network expert (5+ Years of Exp)	1
3.	Security Experts (5+ Years of Exp)	1

Annexure S: Format of Integrity Pact

(To be signed on Plain Paper)
(To be submitted as part of Technical Proposal)

RFP No.: 30-40/2022/USOF/PMU/Part-II; Tender Title: Selection of Managed Service Provider for Migration, Hosting & Operations of IT applications of Digital Bharat Nidhi on MeitY empanelled Cloud

This Agreement (hereinafter called the Integrity Pact) is made on _____ day of the month of _____202__ at _____, India.

BETWEEN

Digital Bharat Nidhi, ---------- through Administrator, for and on behalf of President of India (hereinafter called the "DBN", which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part

AND

M/ s. _____ (hereinafter called the "The MSP", which expression shall mean and include unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

PREAMBLE

'DBN intends to award, under laid down organizational procedures, contract/ s for _____, DBN values full compliance with all relevant laws of the land, rules, regulations, economical use of resources and fairness/ transparency in its relations with its Bidder(s).

In order to achieve these goals, DBN shall appoint Independent External Monitors (IEMs) who shall monitor the Procurement Process and the execution of the contract for compliance with the abovementioned principles.

Section 1 - Commitments of the DBN

(1) DBN commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the DBN, personally or through family members, shall, in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for

self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The DBN shall, during the Procurement Process, treat all Consultant(s) with equity and reason. The DBN shall, in particular, before and during the Procurement Process, provide to all Consultant(s) the same information and shall not provide to any Consultant(s) confidential/ additional information through which the Consultant(s) could obtain an advantage in relation to the Procurement Process or the contract execution.
c. The DBN shall exclude from the process all known prejudiced persons.

(2) If the DBN obtains information on the conduct of any of its employees, which is a criminal offence under the IPC/ PC Act, or if there be a substantive suspicion in this regard, the Principal shall inform the Chief Vigilance Officer and in addition, can initiate disciplinary actions.

Section 2 - Commitments of the 'MSP/ BIDDER(S)'

(1) The 'MSP' commit themselves to take all measures necessary to prevent corruption. The 'MSP commit themselves to observe the following principles during participation in the Procurement Process and during the contract execution.

a. The 'MSP' shall not, directly or through any other person or firm, offer, promise, or give to any of the Principal's employees involved in the Procurement Process or the execution of the contract or to any third person any material or other benefit which he is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the Procurement Process or during the execution of the contract.
b. The 'MSP' shall not enter any undisclosed agreement or understanding with other Consultants, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of Proposals or any other actions to restrict competitiveness or to introduce cartelisation in the Procurement Process.
c. The 'MSP' shall not commit any offence under the relevant IPC/ PC Act; further, the 'Cons MSP' shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the DBN as part of the business relationship, regarding plans, technical proposals, and business details, including information contained or transmitted electronically.
d. The 'MSP' of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any. Similarly, the Con MSP' / Contractors of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details, as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers", shall be disclosed by the Consultant MSP'. Further, as mentioned in the Guidelines, all the payments made to the Indian agent/ representative must be in Indian Rupees only. A copy of the "Guidelines on Indian Agents of Foreign Suppliers" is placed in the Appendix to this agreement.

e. The 'MSP' shall, when presenting their Proposal, disclose any and all payments made, are committed to, or intends to make to agents, brokers, or any of their intermediaries in connection with the contract award.

f. MSP' who has signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The 'MSP' shall not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 - Disqualification from Procurement Process and exclusion from future contracts

If the 'Consul MSP', before award or during execution, has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the 'MSP' from the procurement Process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 - Compensation for Damages

(1) If DBN has disqualified the 'MSP' from the Procurement Process prior to the award according to Section 3, the Principal is entitled to demand and recover from the MSP' the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If DBN has terminated the contract, or if DBN is entitled to terminate the contract, the DBN shall be entitled to demand and recover from the MSP' liquidated damages of the contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) MSP' declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the Procurement Process.

(2) If the MSP' makes an incorrect statement on this subject, he can be disqualified from the Procurement Process, or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 - Equal treatment of all MSP' / Contractors/ Subcontractors

(1) In the case of Sub-contracting, the MSP' shall take responsibility for the adoption of the Integrity Pact by the Sub-contractor.

(2) DBN shall enter into agreements with identical conditions as this one with all Consultants and Contractors.

(3) The MSP' shall disqualify from the Procurement Process all sub-contractors who do not sign this Pact or violate its provisions.

Section 7 - Criminal charges against violating MSP(s)/ Subcontractor(s)

If DBN obtains knowledge of the conduct of an MSP' or Subcontractor, or of an employee or a representative or an associate of an MSP', or Subcontractor, which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal shall inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor

(1) DBN appoints a competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively whether and to what extent the parties comply with the obligations under this agreement.
(2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. The Monitor would have access to all Contract documents whenever required. It shall be obligatory for him/ her to treat the information and documents of the MSP' / Contractors as confidential. He/ she reports to the Head of the Procuring Organisation.
(3) The MSP' accepts that the Monitor has the right to access, without restriction, all Project documentation of the Principal, including that provided by the MSP'. The MSP' shall also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.
(4) The Monitor is under contractual obligation to treat the information and documents of the MSP/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and of Absence of Conflict of Interest. In case of any conflict of interest arising at a later date, the IEM shall inform DBN and recuse himself/ herself from that case.
(5) The DBN shall provide to the Monitor sufficient information about all meetings among the parties related to the Project, provided such meetings could have an impact on the contractual relations between the Principal and the Consultant. The parties offer the Monitor the option to participate in such meetings.
(6) As soon as the Monitor notices, or believes to have noticed, a violation of this agreement, he shall so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can, in this regard, submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action, or tolerate action.
(7) The Monitor shall submit a written report to the Head of the Procuring Organisation within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.
(8) If the Monitor has reported to the Head of the Procuring Organisation a substantiated suspicion of an offence under the relevant IPC/ PC Act, and the Head of the Procuring Organisation has not, within the reasonable time, taken visible action to proceed against

such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word 'Monitor' would include both singular and plural.

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the MSP' 12 months after the last payment under the contract and for all other MSP' 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the MSP' and exclusion from future business dealings. If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above unless it is discharged/ determined by the Head of the Procuring Organisation.

Section 10 - Other provisions

(1) This agreement is subject to Indian Law. The place of performance and jurisdiction is New Delhi.
(2) Changes and supplements, as well as termination notices, need to be made in writing. Side agreements have not been made.
(3) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties shall strive to come to an agreement with their original intentions.
(4) Issues like Warranty/ Guarantee etc., shall be outside the purview of IEMs.
(5) In the event of any contradiction between the Integrity Pact and its Appendix, the Clause in the Integrity Pact shall prevail.

For and on behalf of the Principal

(Name of the Officer and Designation)
(Office Seal)

For and on behalf of 'Consultant.'

(Name of the Officer and Designation)
(Office Seal)
For and on behalf of the Principal
Place
Date

Witness 1:
(Name & Address)

Witness 2:
(Name & Address)