REQUEST FOR PROPOSAL (RFP)
For

Empanelment
of
MeitY Empaneled CSPs or their Authorized Partner
for
offering Cloud Services

For
NATIONAL EDUCATIONAL TECHNOLOGY FORUM (NETF)

RFP No: NETF/CSP/2023/01

NATIONAL EDUCATIONAL TECHNOLOGY FORUM (NETF)
Address: - AICTE HQ, Nelson Mandela Marg,
Vasant Kunj, New Delhi-110070

NATIONAL EDUCATIONAL TECHNOLOGY FORUM (NETF)

Reference no.:	NETF/CSP/2023/01
Name of work	Empanelment of MeitY Empaneled CSPs or their Authorized Partner for offering Cloud Services for NETF
The Currency in which payment shall be made	Indian Rupees (INR)
Start date of issuance/publishing of RFP document	16.02.2023
Date and time of Pre bid Conference and Time	27.02.2023 11:00 AM
Bid queries should reach by	26.02.2023 till 09:00 AM Bid queries received later than the date and time as mentioned above shall not be entertained. Pre-bid queries should be emailed to tenderegov@aicte-india.org
Venue of Pre-Bid Conference	O/o CCO (NEAT), NETF, AICTE HQ, Nelson Mandela Marg, Vasant Kunj, New Delhi 110070
Last date for Online Submission of e-bids	09.03.2023 by 5:00 PM
Date and Time of Opening of Technical Bids	10.03.2023 11:00 AM
Date and time for opening of financial bids	To be intimated Later
Estimated Value of the Project	INR 4.00 Crore
EMD	INR 20.00 Lac (5% of the Estimated Value) in the form of DD in favour of NETF Payable at New Delhi
Tender Fees (non-refundable)	Not applicable as per latest Government Notifications (to be downloaded from the Portal)
Bid Validity days	180 days (From last date of opening of tender)

Chairman (NETF),
National Education Technology Forum (NETF), NETF HQ, Nelson Mandela Marg, Vasant Kunj, New Delhi
tenderegov@aicte-india.org, 011-29581423

DISCLAIMER

The information contained in this Request for Proposal document (the "RFP") or subsequentlyprovided to Bidder(s), whether verbally or in documentary or any other form by or on behalf ofthe National Educational Technology Forum (NETF) or any of its employees or advisors, is provided to Bidder(s) on the termsand conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an Agreement and is neither an offer nor invitation by the NETF to the prospective Bidders or any other person. The purpose of this RFP is to provide interestedparties with information that may be useful to them in making their financial offers (BIDs) pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the NETF in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder mayrequire. This RFP may not be appropriate for all persons, and it is not possible for the NETF, its employees or advisors to consider the investment objectives, financial situationand particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in the Bidding Documents may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations and analysisand should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidder(s) is on a wide range of matters, some of whichmay depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The NETF accepts no responsibility for theaccuracy or otherwise for any interpretation or opinion on law expressed herein.

The NETF, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way for participation in this BID Stage.

The NETF also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. The NETF may in its absolute discretion, but without beingunder any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP.

The issue of this RFP does not imply that the NETF is bound to select a Bidder or to appoint the Selected Bidder, as the case may be, for the Project and the NETF reserves the right to reject all or any of the Bidders or BIDs without assigning any reason whatsoever.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its BID including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the NETF, site visits, investigations, studies or any other costs incurred in connection with or relating to its BID. All such costs and expenses will remain with the Bidder and the NETF shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the BID, regardless of the conduct or outcome of the Bidding Process.

TABLE OF CONTENT

1. General

A. About NETF

National Education Policy 2020 envisage setting up of an autonomous body – National Educational Technology Forum (NETF) to provide a platform for free exchange of ideas on the use of technology to enhance learning, assessment, planning, administration and so on, both for School and Higher Education. The aim of the NETF will be to facilitate decision making on the induction, deployment and use of technology by providing to the leadership of education institutions, State and Central Governments and other Stakeholders the latest knowledge and research as well as the opportunity to consult and share best practices.

B. Background

The NETF has following functions: -

I. To provide independent evidence-based advice to Central and State Government agencies on technology-based interventions;
II. To build intellectual and institutional capacities in education technology;
III. To envision strategic thrust areas in this domain;
IV. To articulate new directions for research and innovation.
V. To lay down standards of content, technology, and pedagogy for online/digital teaching-learning. These standards will help to formulate guidelines for e-learning by States, Boards, Schools, HEIs etc.
VI. To maintain regular flow of authentic data from multiple sources including educational technology innovators and will engage with diverse set of researchers to analyze the data.
VII. To conduct multiple regional and national conferences, workshops etc. to solicit inputs from national and international educational technology researchers, entrepreneurs, and practitioners.
VIII. To Identify technological interventions for the purpose of improving teaching-learning and evaluation process, supporting teacher preparation and professional development, enhancing educational access, and streamlining educational planning, management, and administration including process related to admissions, attendance, assessments etc.
IX. To categories emergent technologies based on their potential and estimated frame for disruption, and periodically present this analysis to MoE.

2. Scope of the Project / Services

NETF has initiated promotional activities related to improvement in Technical Education across the country by way of providing Internship opportunities, industry connect, organizing and various other events of National importance for which web portals are launched.

NEAT (National Education Alliance Technology) for assessment of Students and Industry Institute Collaboration. NETF has currently hosted and is managing its web applications from its own data center. Most applications are developed under Linux/Windows platform with MySQL Database.

As the number of applications are increasing day-by-day NETF plans to host new applications and migrate the existing applications of NETF from current physical servers and azure on cloud in phased manner and use the state-of-art technology to take advantage of upscaling, downscaling and other benefit of cloud technology. The project to be executed for a period of three years initially that can be extended further on the same terms and conditions on mutual agreement.

A. NETF has developed some applications using below technology/Services:

- Node.js, react.js, angular.js, MongoDB, Laravel, Php, mysql and other open source stakes
- Microsoft Translation services API (Cognitive services)
- MS Office 365 enterprise
- CDN (Content Delivery Network) Services
- Video streaming and storage. The Videos so recorded should be automatically stored on NETF server in sync mode while live-streaming.

I. The Supplier shall be responsible for providing the required cloud services and optionally other services (mentioned in this document at various clauses) as per the work order placed by the NEFT and as per the prices discovered through this RFP or as revised downward from time to time.

II. The Supplier should provide at least one dedicated technical resource to NEFT for preparing the technical solution and proposals based on the client requirement.

III. NEFT and NEFT 's end client requires server, storage, database, network bandwidth, and relevant operating system and other services on fully secured cloud environment designedin such a way that guarantee zero data loss. The servers where applications will be hostedcould be anywhere in India but not outside India. This means the data hosted by NETF orNETF's Client should never cross the Indian shores.

IV. Supplier shall provide inter-operability support with regards to available APIs, data portability etc. for the end Client to utilize in case of change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

V. The proposed application cloud environment should provide flexibility to scale the environment horizontally by adding more Virtual Machines of the same configuration to aload balanced pool. It should be possible to scale the solution horizontally at any time, without prior notification to the Supplier or its CSP. It should be possible to automate this process of scaling up and down automatically.

VI. It should be possible at any time to move the Cloud Virtual Machines to Client Data Centre if required. The mechanism and technical requirements for achieving this should be well documented.

VII. The CSP / Supplier should provide all variants of cloud service as mentioned in the Technical Compliance sheet in Annexure N and Annexure O– Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

VIII. The Supplier must initiate the services within 24 hours of placing of work order.

IX. The Supplier would be required to create and maintain a Helpdesk / telephonic number andemail-based ticketing system that will resolve problems and answer queries related to the work order. The supplier shall provide the single point of contact for each client for any support request of the client on 24 x 7 x 365 basis.

X. All terms and conditions of the CSP's empanelment with MeitY are automatically

applicable to this RFP and contract thereof.

XI. DR site should not be in the same premises as DC site. Both DR and DC sites should lie within India.

XII. The SLAs and Penalties would be applicable as per clause 7.8: SLA and Penalties.

XIII. The bidder and the CSP (if the bidder is authorized partner of CSP) must provide the technical compliance as per Annexure N and Annexure O. The Self certified document needs to be submitted during the bidding.

XIV. For all the cloud services being quoted, the bidder has to ensure that all software being offered are genuine and comply to the licensing policy of the software OEM.

B. Scale-up and scale-down of resources

I. Due care would be taken by the Client in deciding the resources and services needed for every requirement. However, the need for increasing or decreasing the resources and services cannot be ruled out. Accordingly, the Client(s) may scale-down the resources or scale-up the resources as per their requirement, subject to below mentioned clauses.

II. All resources can be scaled up or down without any restrictions except the committed resources. The charges for replaced resource would be paid till they have been used. Similarly, the charges for additional resources would also be payable from the time they are put into service as per the rates provided by the Supplier or as revised from time to time.

III. For example, if the Client has taken a "Windows VM – 2 vCPU, 4 GB RAM" and 100GBof "Premium Block Storage (SSD)", then if the Client desires to:

i. Scale down to "Windows VM – 1 vCPU, 2 GB RAM" and 50GB of "Premium Block Storage (SSD)" after 3 months of using the initially ordered resources, then charges for "Windows VM – 1 vCPU, 2 GB RAM" and 50GB of "Premium Block Storage (SSD)"shall be applicable immediately from the time when they are put into active mode and the billing for replaced resources shall be stopped immediately from the time they are replaced.

ii. Scale up to "Windows VM – 4 vCPU, 8 GB RAM" and 200GB of "Premium Block Storage (SSD)" after 3 months of using the initially ordered resources, then charges for "Windows VM – 4 vCPU, 8 GB RAM" and 200GB of "Premium Block Storage (SSD)"shall be applicable immediately from the time when they are put into active mode and the billing for replaced resources shall be stopped immediately from the time they are replaced.

IV. The invoices by the Supplier should clearly indicate such scaling of resources.

V. A prior intimation through mail or letter by Client shall be provided to the supplier whenever scale-down or scale-up (including auto scaling) of resources takes place.

VI. If there is any deviation in the services that are in the work order then the client and the supplier should inform NETF before using any extra services that are nor present in work order.

VII. The prices with the scaled-up or scaled-down resources would be reflected in all future

invoices.

VIII. In case the Client does not have skilled resources or expertise to migrate to cloud or manage the provisioned environment, the Client can procure services mentioned in clauses of this RFP.

IX. However, even if the Client procures other Services mentioned in clauses of this RFP from the Supplier, in view of the shared responsibility, it is essential that the Client:

i. Monitors the operational activities to have the complete view into the provisioned cloudservices and their configurations.

ii. Review and validate the security configurations, review the notifications and patchesreleased by the CSP.

iii. Have the visibility into the provisioned infrastructure (including the utilizations) so thatthere is no over-provisioning leading to excess payments to the Supplier.

X. The Supplier in consultation with the Client and NETF will strive to optimize the provisioned resources by understanding the usage patterns and recommending terminationof the under-utilized instances through continuous optimization. The Supplier / CSP is required to give timely suggestions for achieving such optimizations.

XI. The Client may also discuss the possibilities of application re-engineering using advanced cloud features (e.g., auto-scaling, content delivery network) and additional PaaS services where possible to get further cost optimizations (e.g., Move large blob object and media files to Object storage and store a pointer in your existing database; migrate archival data to cold storage, etc)

C. Disaster Recovery Services

The supplier shall provide business continuity and disaster recovery services to meet the RPO and RTO as per the service levels. In case the primary environment goes down, the Supplier shall scale up the DR environment for the services to be delivered without any effect on the performance. DR should be provided by the CSP. The following should be followed:

Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) Change over from DC to DR or vice versa.	RTO <= 4 hours
Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours

D. Migration Services

I. Migration Services are not a part of Cloud Managed Services (Refer relevant Clauses) and will have to be taken separately even if Cloud Managed Services have been opted. If the Client does not have expertise to migrate their existing applications to Cloud, the Client can

procurethe cloud migration services from the Supplier which shall include the following:

II. Application and Infrastructure Discovery & Portfolio Analysis:
   i. Formulate a baseline of the Client's technical environment including inventory of both applications and infrastructure. This should also include development/testing environments in addition to the production environment.
   ii. Document the technical details of the applications including technical architecture, integration with external solutions, underlying technologies / platforms, and underlyingsoftware. For each of the applications, capture the logical and physical deployment architecture providing the details of various architectural components (e.g., load balancer, firewall).
   iii. Identify the applications and their dependencies on other components and services. Create a dependency tree that highlights all the different parts of the applications and identify their upward and downstream dependencies to other applications.

III. Define TO BE and Security Architecture for Cloud
   i. Estimate the resources required on cloud based on the application, current / anticipatedserver, storage configurations and workloads.
   ii. Define the indicative or the minimum requirements need to be provided for each kind of environment (Development, QA, Training, Staging, and Production - as applicable for the project) that is planned on cloud.
   iii. Supplier should propose and, in consultation with the department, finalize the security architecture for the workloads being migrated to cloud.
   iv. Define the logical architecture indicating the different compute, storage, network, security and monitoring services that will be provisioned for deploying the application on cloud.

E. Cloud Managed Services

I. In case the Client, does not have capacity to manage the provisioned cloud services, the Client can procure the cloud managed services (e.g., provisioning, security configuration, monitoring) from the Supplier.
II. These services exclude Migration Services which need to be procured separately by the Client.
III. The Exit Management services as defined in the RFP (as per relevant Clause) shall be the responsibility of the supplier.
IV. The scope of Cloud Managed Services includes the following: -
   i. Resource Management: Adequately size the necessary compute, storage and other cloud services required, building the redundancy into the architecture and load balancing to meet the service levels. Based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute and storage asper the performance requirements of the solution. The scaling up / scaling down (beyondthe auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by end client and NETF.

ii. Patch & Configuration Management (Remote OS Administration): Manage the instances of compute, storage, and network environments. This includes department-owned & installed operating systems and other system software deployed by the Supplier.

iii. User Administration: 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. Implement multi-factor authentication (MFA).

iv. Security Administration: Configure, monitor and regularly review the security services / configurations for the workloads deployed on Cloud. Monitor the environment for unauthorized activity / access to the systems and conduct regular vulnerability scanningand penetration testing of the systems.

v. Monitoring Performance and Service Levels: Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.

vi. Backup (if procured by the Client): Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by Client. Restore from the backup where required.

vii. Training: Provide training to the officials of the Client on request. The training may be provided online or offline as per the requirements of the Client. The infrastructure for the offline training will be provided by the Client.

viii. Support for third party audits: Enable the logs and monitoring as required to support forthird party audits.

ix. Miscellaneous: Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloudservices, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

x. Provide the regular reporting to the Client: Security assessment report with respect to security configuration gaps and possible improvements to the security and compliance of cloud services on a quarterly basis. In case any gaps / scope for improvement are identified, the same needs to be discussed with the Client and resolved in mutual consultation with the Client, either as fixed and hence no longer a gap or acceptable risk and hence no further action required.

F. Cloud Advisory Service

I. If the Client does not have expertise in Cloud Services, the Client can procure the cloud advisory services from the Supplier which shall include the following:

i. Cloud Infrastructure Advisory Service: Supplier will examine the different models

which can be used within organization for delivery – public, private and hybrid cloud. the current cost of existing environment (status quo) is examined and a total cost of ownership (TCO) calculation for a cloud-first environment is provided. Supplier will provide an in-depth examination of current infrastructure and how current infrastructureneeds to change and develop if it's moved to the cloud. This will allow client that whattheir environment will look like when running in the cloud. This service provides a fullROI picture of the impact of a cloud migration for an organization.

ii. Migration assessment services: Supplier will design a successful migration roadmap based on application dependencies, suitability, and readiness – while ensuring cost-performance optimization is considered the moment you are ready to migrate your servers and applications to the cloud.

iii. Cloud Optimization services: Most public cloud client pay more than what they utilize. The cost can be reduced by optimizing the infrastructure utilization. Each component ofCloud server, storage, tools and other services has to be reviewed. Integrating Cloud Optimization services will allow the TCO to be brought down overall. The cost can be reduced without compromising on availability and performance. Supplier will provide cost optimization methods of the solution by studying the current utilization.

iv. Cloud Security Audit Services: Supplier will Identifying the potential security vulnerabilities. how to prevent future attacks using audit tools. Suggest and develop strategies for protection from attacks and take measures against potential failures, by using trending security and monitoring tools with proficient automation.

G. Cloud Capacity Building Services

I. Supplier will provide online and offline training on cloud services mentioned in technical compliance of Annexure.

II. The Supplier will take attendance and feedback after the training for the invoicing purpose.

H. SLA and Penalties

The key service level objectives that relate to the cloud service and the related aspects of the interface between the department and the cloud service provider are indicated below:

I. The SLA parameters shall be monitored on a monthly/quarterly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of Client, then the NETF will have the right to take appropriate disciplinary actions including termination of the contract.

II. The full set of service level reports should be available to the Client and NETF on a monthly/quarterly basis or based on the project requirements.

III. In case these service levels cannot be achieved at service levels defined in the agreement, NETF shall invoke the performance related penalties. Payments to the Supplier will be linked to the compliance with the SLA metrics laid down in the agreement.

IV. In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a

sum of penalties for the applicable SLA violations.

V. GST as applicable shall be charged on the Penalties on SLA's.

VI. Penalties shall not exceed 100% of the monthly/ quarterly bill. If the penalties exceed more than 50% of the total monthly/quarterly bill, it will result in a material breach. In case of amaterial breach, the Supplier will be given a cure period of one month to rectify the breachfailing which a notice to terminate may be issued by the Client.

S.No.	Service Level objective	Measurement Methodology	Target/Service level	Penalty
Availability/Uptime				
1.	Availability/Uptime of cloud services	Availability (as per the definition in the SLA)	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resources will attract penalty as indicated below.
				• < 99.5% & >= 99.25% (10% of the Monthly/ quarterly Payment) • < 99.25% and >= 99.00% (20% of the Monthly/quarterly Payment) • <99.00% (30% of the Monthly/ quarterly Payment) • In case the services are not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Monthly/Quarterly Payment of the Project.
Support Channels – Incident and Helpdesk (as per Clause 7.1.XI)				

2.	Response time	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.	95% within 15 minutes	< 95% (1% of the Monthly/ quarterly Payment for each percentage drop below 95%)
3.	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 99% of the incidents should be resolved within 30 minutes of problem reporting	• < 99% & >= 97% (5% of the Monthly/ quarterly Payment) • < 97% & >= 95% (10% of the Monthly/ quarterlyPayment) • < 95% (15% plus 1% of the Monthly/ quarterly Payment for each percentage drop below 95%)
4.	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of severity 3 within 16 hours of problem reporting	• < 95% & >= 90% (2% of the Monthly/ quarterly Payment) • < 90% & >= 85% (4% of the Monthly/ quarterly Payment) • < 85% (6% plus 1% of the Monthly/ quarterly Payment for each percentage drop below 85%)

VII. Maximum cumulative penalty cannot exceed 10% of the work order value after which theNETF may cancel the work order and forfeit the Performance Security submitted by the Supplier. This cumulative penalty cap is hit twice against various work orders, then NETF will forfeit all the Performance Security submitted by the Supplier and may also lead to termination of the contract.

VIII. The above-mentioned SLAs are subject to the client requirement. If client request for morestringent SLA's, then it is responsibility of the bidder to provide the SLAs at no extra costto NETF.

IX. Severity Levels

i. Below severity definition provide indicative scenarios for defining incidents severity. However, NETF will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

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 andcritical 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.	

3. Documents required to be submitted along with the technical bid The bidder should submit the following documents as part of bid:

The bidder is requested to submit the following documents offline to the O/o CCO (NEAT), NETF, AICTE HQ, Nelson Mandela Marg, Vasant Kunj, New Delhi 110070 before the start of Public Online Tender Opening Event in a Sealed Envelope bearing the project name, the tender number and the words 'DO NOT OPENBEFORE' (due date & time).

a. Original copy of the EMD Security in the form of Demand Draft
b. Original copy of the power-of-attorney.

Note: The Bidder must also upload the scanned copies of all the above-mentioned originaldocuments as Bid-Annexure during Online Bid-Submission.

The Online Technical Bid (.PDF complete in all respect) must be uploaded online as explained below: -

Annexure A – Declaration Sheet format
Annexure B – Letter of Undertaking
Annexure C – Power of Attorney
Annexure D - Performa for Declaration from bankon Proceedings Under Insolvency and Bankruptcy Code, 2016
Annexure E - Undertaking for Non-Blacklisting
Annexure F - Technical Bid Submission Letter
Annexure G - Eligibility Criteria
Annexure H - MeitY empanelled CSP Authorization Form
Annexure I - Annual Turn Over Form
Annexure J - Technical Evaluation Criteria
Annexure K – Data Centre Location Certificate
Annexure L – Technical Compliance for CSP Services

4. Responsibilities of Bidder/Cloud Service Provider:

The cloud service provider shall be responsible for following:

I. Bidder shall be responsible for setting up, installation, configuration, management, upgradation, and migration of application servers, database servers/storage.

II. Maintain and manage the required network components for the cloud services procured by NETF. Setup and configure the VMs, storage, Network, Database etc. at DR site meeting RPO and RTO (Recovery Time Operations) requirements of NETF Service provider shall provide access to logs for analysis.

III. Service provider shall not delete any data before without approval of NETF during the period of Contract and will not delete any data after the expiry of Contract without written approval from NETF.

IV. Service provider shall be responsible for implementation, management and monitoring of DDOS, IPS, IDS Services, etc.

V. Service provider will implement anti-malware and conduct regular vulnerability scanning and penetration testing of systems and infrastructure.

VI. Service provider shall have public Services in DMZ zone and High security services in MZ Zone.

VII. Service Provider shall configure external connections to the hosting infrastructure required to upload database/files etc.

VIII. Service provider is expected to understand the complete architecture of existing applications and processes necessary for smooth migration of applications and databases including interdependencies between applications and data.

IX. Service provider shall be responsible for deployment of Security patches on Hardware and Software.

X. Bidder will be responsible for migrating to cloud and managing the cloud services.

XI. The bidder shall be responsible to monitor the cloud services and ensure 99.9 % uptime of all services as per agreement.

XII. Establishing connectivity between NETF's premises to cloud DC and DR site.

XIII. Deployment of New Applications on cloud, security administration, planning and implementation of cloud management and monitoring portals for complete infrastructure and services procured.

XIV. Bidder shall be responsible for monitoring and reporting services.

XV. Bidder shall provide 2 Cloud engineers/cloud professionals initially for a period of one year on site at NETF Headquarters.

XVI. Provide access to NETF for installation/commissioning and management of Virtual Machines.

XVII. Provisioning of scalable storage capacity as per requirements of NETF and availability of such services as per agreement.

XVIII. Service provider shall ensure committed time taken for restoration of data from Backup as claimed.

XIX. Service provider should ensure and meet all standard data formats for data transfer /portability from cloud to NETF machines and vice-versa.

XX. Service provider shall demonstrate/Submit documentary proof for POC (Proof of Capability) as part of technical evaluation to understand the key features such as AUTO Scale up/down, Security protocols, Denial of Service (DoS, DDoS) attack), management and administration and audit capabilities of offerings, setting up of DR facilities, etc.

XXI. Service Provider shall provide inter-operability support with regard to APIs and Data Portability.

XXII. Service provider shall be responsible for security of Facilities, Physical Security of Hardware, Network infrastructure and virtualization Infrastructure.

XXIII. Service provider shall be responsible for any Risk Management and planning, or issues related to migration of data from DC to DR.

XXIV. Service Provider shall be responsible for managing services provided by third party vendors.

XXV. Service provider shall workout migration plan for co-existence of non-cloud and cloudarchitecture during and after the migration period in close coordination with NETF.

XXVI. Service provider shall provide necessary training to NETF or its Systems Integrator on management of cloud VMs.

XXVII. Service provider shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services.

XXVIII. All risk management related to migration, migration plan shall be jointly worked out with NETF and Cloud Service Provider.

XXIX. Service provider shall have provision to provide and support additional VM requirements and related services.

XXX. Service provider shall assist NETF in planning for capacity building to meet growth and peak load assessment at the end of first year to ensure future requirements of NETF are addressed.

XXXI. The service provider shall provide necessary details including sizing, current loads, utilization, expected growth/demand and other details for scale up/scale down at the end of first year in close coordination with NETF.

XXXII. Service provide shall provide Annual Technical Support from OEM under (Software procured as PaaS) during entire period of Contract.

XXXIII. NETF and Service provider shall jointly workout multi-factor authentication for root account as well as any other privileged identity and access account associated with it.

XXXIV. Service provider shall be responsible for implementation of tools and processes for monitoring the availability of applications, responding to system troubleshooting.

XXXV. Monitoring of performance, resource utilization and other events such as failure of services, degradation of services, availability of network, storage, Database systems, OS etc.

XXXVI. Provide the relevant reports, including real time as well as past data/reports on dashboard.

XXXVII. Service provider shall be responsible for conduct of DR Drills and follow Standard Operating Procedures (SOP) and inform NETF in advance for such drills conducted twice a year normally, with 15 days' prior notice.

XXXVIII. There should not be any data loss during backup from DC to DR.

XXXIX. Service Provider shall monitor Internet Links, MPLS -VPN including bandwidth, data transfer, response time and packet loss and perform corrective measures.

XL. After the implementation of exit process, cloud service provider will delete/remove VMs, contents and data with approval of NETF and ensure data cannot be forensically recovered and intimation of compliance thereafter.

XLI. The Service Provider will train and transfer the knowledge to the replacement agency or NETFto ensure continuity and performance of services post expiry of Contract.

5. Role of NETF/ NETF's Systems Integrator

I. NETF/ NETF's System Integrator shall be responsible for management of all NETF webapplications hosted on Service provider's platform/Data Center.

II. NETF shall be responsible for all web application SLA with systems Integrator.

III. NETF shall be responsible for design/development and management of all web applications.

IV. NETF shall be hosting applications on Service provider's platform which include application configuration, addition and deletion of modules and ensure application functionality as per end user's requirements.

V. NETF shall be responsible for planning and sizing of applications along with its architecture.

VI. NETF shall be responsible for remote administration of applications on VMs provided by Service provider through VPN.

VII. NETF will estimate the requirements of Infrastructure resources (like VMs, Storage etc.) for different environments such as production, pre-production (non-live environment), test environment etc.

VIII. NETF will work out minimum resource requirements as well as indicative requirements of services like IP address/Load/Data transfer in Local and DR site etc.

IX. NETF shall also share with service provider the listing of existing Software licenses already procured by NETF (OS/DB…) including its upgrades if any, and if required.

X. In case of New Projects NETF will procure software licenses or may procure/ subscribe the minimum required licensees as part of PaaS (Platform as a Service)

XI. NETF will specify additional Security requirements for some applications like PCI-DSS. Data Encryption, Third Party authentication support (e.g. e-sign/Digital signing Certificates) for Payment gateway requirements.

XII. NETF shall define the data retention period for all applications as per need basis application- wise.

XIII. NETF shall define the Log retention policy, application-`wise as per need.

XIV. NETF shall work out estimated size of data for backup wherever possible.

XV. NETF shall be responsible to conduct of regular vulnerability scanning and penetration testingof applications and fixing up of such vulnerabilities.

6. Pre-Bid Conference

The queries should necessarily be submitted in the following format:

RFP Description	

RFP No.			
Organization			
Address			
Contact Person			
Contact No.			
Mail Id			
S. No.	PageNo	Clause as perRFP	Clarification Sought

7. General Conditions

S. No.	Item Description
1	Monitoring tools shall not capture or send NETF data to any other establishment over Cloud.
2	The E-BIDDER shall have to enter in SLA (Service Level Agreement) with NETF. E-BIDDER should have ability to Integrate with Digital Certificate/signature and other similar services like email/SMS obtained by NETF from Third party.
3	The ownership of Data as well as application shall be of NETF and NETF can ask for fullcopies of Data and applications at any time.
4	E-BIDDER shall provide complete inter-operability support with regard to available APIs, data Portability, application portability in case NETF decides to Change the cloud service provider including DR or backups.
5	No data shall be shared with any Third Party without written approval of Competent Authority of NETF unless legally required by Court Orders.
6	E-BIDDER shall be responsible for managing and controlling the underlying cloud infrastructure including O.S, Storage, network, Security. Deployed Applications shall be managed and controlled by NETF
7	As part of PaaS the e-Bidder shall provide all necessary technical support for backend infrastructure like O.S, Databases etc.
8	Prior Intimation (at least 15 days) shall be given to NETF by Service provider for any scheduled maintenance of servers.
9	The E-Bidder shall be responsible for all upgrades of Operating systems, Database and related tools including patch management.
10	CSP/E-BIDDER shall have to enter into non-disclosure agreement with NETF for data/documents stored on Data Centre.
11	SLA shall have exit Clause based on mutual Terms and conditions.
12	E-BIDDER shall be responsible for Data and Application Migration of existing applications, which NETF would like to migrate to new environments of cloud. Necessary requirements shall be shared by NETF in phased manner.
13	E-Bidder shall be responsible for deploying new applications on Cloud, user administration, security administration, planning and implementation with monitoring tools for infrastructure and Services procured.
14	The e-Bidder shall ensure minimum Three years of services extendable with mutual consent with exit clause in SLA.
15	The Billing Cycle shall be quarterly and services to be quantified on monthly

	subscription/ utilisation basis.
16	NETF may or may not seek all services in one go, however, E-BIDDER shall provide the services on demand basis for which Billing shall be from the date of initiation of such services and actual utilisation.
17	The E-Bidder shall provide along with Invoices, consumption report to supplement the Invoices.
18	Appropriate penalty shall be applied as per Service Level Agreement mutually acceptable toNETF and Service provider.
19	The development and testing requirements may be different than production requirements, hence upscaling and downscaling should be possible.
20	Service Provider should be able to provide load balancing for proper distribution of traffic.
21	The load balancing should be l supporting Database as well.
22	Services providers should be in position to provide DR Services.

8. Requirements of NETF on cloud

IaaS services				
S.NO	VM NAME	OPERATING SYSTEM	SIZE	DISKS
1	AICTEFIVM	Linux	Standard_E16s_v3	2
2	AICTEINTVM01	Linux	Standard_E16s_v3	2
3	AICTENATSWEB01	Linux	Standard_E16s_v3	2
4	AICTEIITMD1	Linux	Standard_D16s_v3	1
5	AICTEIITMD2	Linux	Standard_D16s_v3	1
6	AICTEHELPVM1	Linux	Standard_D32ds_v5	1
7	NEAT-CELL-DEV-VM	Linux	Standard_E16s_v3	2
8	NEAT-CELL-TEST-VM	Linux	Standard_E16s_v3	2
9	AICTEHELPVM2	Linux	Standard_D16s_v3	1
10	debugvmwin-V2	Windows	Standard_E16s_v3	2
11	ONODAPPBE01	Linux	Standard_E16bds_v5	2
12	ONODAPPFE01	Linux	Standard_E16bds_v5	2
13	ONODDB01	Linux	Standard_E32ds_v5	2
14	voiceqabe01	Linux	Standard_D4ds_v5	2
15	voiceqadb01	Linux	Standard_D4ds_v5	2
16	voiceqafe01	Linux	Standard_D4ds_v5	2
PaaS Services				
	NAME	RESOURCE TYPE	SIZE	
1	NETFhelpdb	Database for MySQL single server	General Purpose, 64 vCore(s), 1334 GB Storage (Auto growth)	
2	Natsmysqldb	Database for MySQL flexible server	General Purpose, D16ds_v4, 16 vCores, 64 GiB RAM, 128 storage, 1000 IOPS	
SaaS Services				
1	Twilio SendGrid - Pro 300K			

Cognitive service				
	NAME	KIND	TIER	
1	SpeechServices	Speech Services	S0	
2	Translator	Text Translation	S1	
Application gateway (WAF V2)				
	NAME			
1	AHAPPGTW			
2	NETF_AppGW			
3	ZSIND-NETF-PRD-MOENATS-AGW			
	VM series	Configuration		
1	L32 (initial 20 Qnties required)	256 GB NVMe RAM, 32 Core, 51200 iOPS		

A. Services required

I. VMs as above with Linux/Windows Platform
II. Linux box with Angular.js, Laravel, Php, mysql, node.js, server with apache/nginix/iis anyversion php version greater than or equal to 7.0.
III. Database: MYSQL/MONGO DB /Postgre SQL or any other open-source Database
IV. Backup of Database and applications Locally and on DR
V. Inter and Intra Region Data Transfer
VI. Bandwidth
VII. Log Analysis
VIII. Disk Read/Write operations
IX. Static and Dynamic IPs
X. VPN services
XI. Dash Board for NETF administrator for Monitoring VMs and reports, Utilisation of resources.
XII. Load Balancing
XIII. Web application Firewall(WAF) Services.
XIV. Anti-Virus and patch management
XV. Domain URL mapping
XVI. Any other relevant services which may be required in future

Note: *Model to be used: "Pay as You Go" on monthly consumption basis.

B. Basic Service:

S. No.	Service Category	Minimum Requirement for compliance
1.	Compute	• Must support variety of operating systems including: Linux, Ubuntu, Windows Server, RedHat Enterprise Linux, SUSE Linux Enterprise Server, openSUSE Leap, Fedora, Fedora CoreOS, Debian, CentOS, Gentoo Linux, OracleLinux, and FreeBSD • Should be capable to deploy across multiple datacenters • Should support autoscaling on the basis of CPUutilization • Platform should have capability to spin upthousands of instances in minutes • Should provide Intel, AMD based processor • Should support block storage and temporary block storage (to store Information that changesfrequently, such as buffers, caches, scratch data,and other temporary content) • Also support Block Storage Encryption

2.	Storage	• Block Storage
		  • Block Storage must provide 99.9% SLA
		  • Block Storage should support volumesnapshot
		• Object storage
		  • Object Storage must provide strong readafter write consistency
		  • Object Storage should unlimited scalestorage.
		  • Object Storage must support intelligent data tier on the basis of data use. Also have built in capability to analyze storage accesspatterns to help you decide when to transition the right data to the right storage class
		  • Object Storage supports versioning andMFA for deletion.
		  • Object storage should have integration withHSM to provide inherent capability of encryption

		• File Storage • File Storage should span across multipleavailability zone • Backup Storage • Archival Storage • Retrieval of Archival Storage • All the storage supports Data Encryption
3.	Network	• Isolated Network defined at regional level mustbe able to span to multiple availability zones • Private network connectivity between VPCs,services, and on-premises applications • Securely deliver data, videos, applications, and APIs to customers globally with low latency, andhigh transfer speeds • Should have capability to communicate withobject storage using private network • Also supports private link between on promise tocloud infrastructure • Should provide Native Firewall with Stateful andstateless rules along with IPS capability.

4.	Security	• CSP must provide native service for security like
		• Identity & access management
		  • Manage user access and encryption keys
		  • Single Sign on Service for Cloud
		  • Centralize Governance and ComplianceManagement
		• Detection Control
		  • AI Powered Threat Detection Service
		  • Unified Security and ComplianceDashboard
		  • Vulnerability Assessment
		  • Record and Evaluate Configuraion
		  • Track API and User Activity
		• Infrastructure Protection
		  • Network Firewall with IPS capability
		  • Web Application Firewall
		  • DDoS protection
		  • Central Management of Firewall Rules
		• Data Protection:
		  • Sensitive Data Discovery and Protection
		  • Encryption Key storage and KeyManagement (FIPS compliant)
		  • FIPS Compliant Fully managed scalableHardware Security Module
		  • Centralize Provision, manage, and deploypublic and private SSL/TLS certificates
		  • Central Store to Encrypt, Rotate, manageand retrieve secrets
		• HSM
		  • Should support FIPS 140-2 Level 3 for thestorage of encryption keys ssl certificates etc. as managed service
		  • Should provide managed backup service for HSM Cluster to provide ability of restoration of keys in case of any failure ofHSM device
		• Incidence response
		  • Potential Security Threat InvestigatingControl
		  • Fast and Automated Control for DisasterRecovery and Ransomware Recovery

5.	Management andGovernance	•Automate, configure and update your resources •Must have capability to enforce organizationlevel security compliance and governance •Should have capability to ensure continuouscompliance •Should trigger events and alerts on non- conformance on defined organization level governance and should have capability preventthe configuration changes.
6.	Monitoring and Alert Management	•Should provide detail monitoring of resourcesand services •Should have capability to define custom alertsand matrices for resources •Ability to store log and analyse logs using SQLquery statement. •Must have capability to trigger events, alerts andalarm •Must provide capability to automate
7.	Migration	•Database Migration Service should supporthomogeneous and heterogeneous database replication •Storage Transfer Service should provide capability to extend on premise application to cloud storage, also provide capability for petabyte scale data transfer

C. Advance Services:

S. No.	Service Category	Minimum Requirement
1.	Containers	•Share and deploy container software, publicly or privately •Manage containers withKubernetes •Should provide private or publicdedicated container registry to store , deploy and share the containers •Should also provide platform torun container without managingservers •Should also help to containerizeand migrate existing application •Cloud service should support deployment of Docker containerwith orchestration (Kubernetes/any native orchestration System)
2.	Serverless	•Should be managed Platform •Should provide capability toscale zero to peak demands •Must have built in fault toleranceand support event driven architecture •Must have set of native servicesavailable to enable communication between decoupled components within microservices, distributed systems, and serverless applications. •Must have serverless backend (compute, integration, and data stores) to run serverless workload
3.	Managed Database Services	•It should be cloud managed platform for following database • RDBMS (MS SQL server,MySQL, Postgresql, MariaDB) • Graph Database • Blockchain Database • NoSQL Database • In Memory Database • MongoDB CompatibleDatabase •All the database platform supports high availability andfault tolerance •All these database platformsshould be scalable •Must provide auto scalable serverless platform for MySQLand PostgreSQL •All these databases must supportencryption for data at rest and data in transit. •Database platform must supportmulti-region, multi-master replication •Database platform must providefull oversight of your data with multiple

		levels of security, including network isolation, andend-to-end encryption
4.	DevOps	• Automatically build, test, distribute, deploy and monitoriOS, Android, Windows and macOS apps—all in one place • Developers can regularly merge their code changes into a central repository, after which automatedbuilds and tests are run. • Must provide fully managed service to implement end to end CICD pipeline • Should securely store and versionapplication's source code and automatically build, test, and deploy the application

5.	Analytics & Visualisation Services	• Should provide managed andnative service platform for
		  • Interactive Analytics
		  • Big Data Processing
		  • Real time analytics
		  • Operational Analytics
		  • Data Visualization & Visual Data Preparation
		  • Real Time Data Movement
		  • Predictive analytics andMachine Learning
		• Analytics service should be serverless - No need to provisionor maintain any servers. There isno software or runtime to install,maintain, or administer.
		• Should have built-in availabilityand fault tolerance.
		• Ingest, buffer, and process streaming data in real-time toderive insights in seconds or minutes
		• Handle any amount of streamingdata and process data from hundreds of thousands of sourceswith very low latencies
		• Securely stream video from connected devices for analytics,machine learning and other processing
		• A built-in suggestion engine thatprovides users with recommended visualizations based on the properties of the underlying datasets.
		• Share business insights by packaging them up as interactivestories that users can share with others.

6.	AI and machine learning	• Cloud service should support provisioning. Managed Service/Notebook for writing/training and support various python/R based ML library like Tensorflow, SCi-Kit,Pytorch, XGBoost • Cloud service should support Services for deploy Trained MLalgorithm for inferencing • Cloud service should supportmanaged ML API for Translation, Speech, Image/Video Analysis • Must have ready-made AI capability which can be easilyintegrated with available appsand workflow for enhance business out come • Must provide capability to build,train, and deploy ML models • Should provide platform like Tensor Flow, PyTorch, Apache MXNet, and other popular frameworks to experiment with and customize machine learningalgorithms
7.	Internet of Things	• Should be fully managed nativeservices • Support billions of devices and trillions of messages, and can process and route those messagesto other devices reliably and securely • Connected devices can trigger events, execute predictions based on machine learning models, keep device data in sync, and communicate with other devicessecurely even when not connected to the Internet • Also have capability to run and operationalize sophisticated analytics on massive volumes of IoT data • Should provide facility to securethe IoT devices • Should Provide facility to easy tocollect, store, organize and monitor data from equipment's tohelp in data-driven decisions. • Should provide capability to easyto visually connect different devices and web services to build IoT applications

8.	Application integration tools	• Must provide native control andcapabilities to
		  • Create, publish, maintain, monitor, and secure APIs atany scale for serverless workloads and web applications
		  • Create a flexible API to securely access, manipulate, and combine data from one or more datasources
		  • event-driven architecture
		  • Reliable high throughputpub/sub
		  • Should support No CodeAPI Integration
		• Should provide managed workflow platform like ApacheWorkflow

9.	Hybrid cloud	• Should help to run and manage applications wherever they mayneed to reside • It must provide infrastructure, APIs, services, and tools wherever applications may needto reside to meet low latency, local data processing, or data residency requirements. • Should have native service available to build secure andcompliant hybrid cloud architectures • Should also support cloud nativeInfrastructure services, API and tools to work seamlessly on- premise and cloud.
10.	Media	• Fully Managed service which supports transport, prepare, process, and deliver live and on-demand content This CSP should have services that allows the customers to build intelligent video analytics solutions that can be deployed on cloud. • Should provide capability to integrate with 3rd Party Platformfor media

		storage, machine learning, content protection, monetization campaigns etc.
11.	Mobile/Mobile Applicatio nDevelopment Requirement	• It should be fully Managed Services to create, configure, andimplement scalable mobile applications • Should supports user sign-up,sign-in, and access control to your web and mobile apps. • Must support social identityprovider and custom identityprovider • Cloud service should support provisioning of Backend no SQLdatabase for mobile application • Cloud service should support provisioning of Object Store to support uploading of binary files • Cloud service should support feature of Static Web Contenthosting
12.	Big Data	• Should provide managed platform for processing vast amounts of data using open source tools such as Apache Spark, Hivc, HBase, Flink, Hudi and Presto • Should have capability to runpetabyte-scale analysis • Should also provide Platform for Data Visualization & Visual Data Preparation , Real Time Data Movement and Machine Learning

D. Specialized Services and Licensing

The cloud services provider/bidder should be capable of providing the following services as NETF has developed some applications using below technology/Services:

I. Microsoft Translation services API
II. Bulk email services
III. MS Office 365 enterprise
IV. Supports online Video streaming, storage and Archival like PowerApp Studio or similar Tools.
V. CDN (Content Delivery Network) Services

Note: *The above requirements are indicative and NETF has the right to increase/decrease during the implementation process as per need. During the Technical Evaluation the vendor shall host one of the above application/services on the cloud and will demonstrate the successful functioning of the application.

9. Service Level Agreement:

The bidder shall be required to enter into SLA (Service Level Agreement) which will clearly define the roles/responsibilities and other clauses as applicable and acceptable by NETF and Bidder**.**

10. Performance Security Deposit

The successful bidder shall have to deposit a Performance Security Deposit of the 10% of the total amount of work order within **15 days** of the receipt of the LOI/Order. The performance security deposit will be furnished in the form of Demand draft drawn in favor of **NETF.** The performance security deposit should be valid for sixty days beyond the date of completion of all contract obligations/warranty period.

11. Terms of Payment

The payment shall be made on submission of the bills on quarterly basis. The bill submitted by the bidder should be duly certified by the concerned project officer of NETF. No advance payment will be made. Payment

shall be made only on the basis of actual consumption of services, duly supported with the requisite details of services and consumption report.

Invoice (i.e. Tax invoice as per Service Tax rules clearly indicating Tax registration number, Service Classification, rate and amount of Tax shown separately). The Service provider will submit a bill, in the name of NETF . No claim for interest will be entertained by the NETF in respect of any payment/deport which will be held with the NETF due to dispute between NETF and Service provider or due to administrative delay for the reasons beyond the control of NETF.

All Taxes as per applicable by Govt. of India from time to time will be deducted from all payments made by NETF. The payment is mandatory through NEFT/RTGS only.

12. Exit Management Clause

I. NETF intends to use cloud services provided by the service provider for a period of 3 years and service provider shall enter into a 3-year contract agreement with NETF initially. However, NETF reserves the right to terminate the contract at any point of time without any explanation by giving 3 months' notice.

II. The bidder shall be responsible for providing the tools for import / export of VMs & content on offline physical storage devices, as agreed by NETF, and shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition at no extra cost.

III. In the event of change of accreditation of bidder (Lower accreditation, losing partnership) NETF reserves the right to terminate the contract.

IV. The bidder is responsible for both Transitions of the Services as well as Migration of the VMs, Data, Content and other assets to the new environment at no extra cost.

V. The format of the data transmitted from the cloud service provider to the new environment created by NETF or any other Agency should leverage standard data formats. On expiration / termination of the contract, Bidder will need to handover complete data in the desired format to NETF which can be easily accessible and readable without any additional cost to NETF. Data so received should be transportable to any other Public/Private cloud.

VI. The bidder shall carry out the migration of the VMs, data, content and any other assets to the new environment created by NETF or any other Agency (on behalf of NETF) on alternate cloud service provider's offerings to enable successful deployment and running of NETF solution on the new infrastructure including software licenses at no extra cost.

VII. The bidder shall ensure that all the documentation required by NETF for smooth transition (in addition to the documentation provided by the Cloud Service Provider) are kept up to date and all such documentation is handed over to NETF during regular intervals as well as during the exit management process.

VIII. If the bidder fails to meet the guidelines & standards as set by Government of India and NETF.

13. General Instructions/Terms and conditions

I. While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisors in relation to this RFP.

II. All information supplied by Bidders may be treated as contract binding on the Bidders, on successful award of the assignment by NETF on the basis of this RFP.

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

IV. NETF reserves the right to cancel this public procurement at any time prior to a formal written contract

being executed by or on behalf of NETF

V. This RFP super cedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

VI. Examination of RFP Documents in preparing the proposal, Bidder is expected to examine in detail the documents comprising the RFP. Material deficiencies in providing the information requested in the RFP documents may result in rejection of a Proposal.

14. Conflict of Interest

NETF requires that Bidder provides professional, objective and impartial advice and at all times hold the NETF interest's paramount, avoid conflicts with other assignments or their own corporate interests and act without any consideration for future work. Bidder shall not be recruited for any assignment that would be in conflict with their prior or current obligations to other clients,or that may place them in a position of not being able to carry out the assignment in the best interest of NETF. Without limitation on the generality of the foregoing, Bidder and any of their associates shall be considered to have a conflict of interest and shall not be recruited under any of the circumstances set forth below:

I. If there is a conflict among implementation, operation and maintenance of IT Integrated solution assignments, the Bidder (including its personnel and sub-consultants) and any subsidiaries or entities controlled by such Bidder shall not be recruited for the relevant assignment.

II. A Bidder cannot be recruited to carry out an assignment that, by its nature, will result in conflict with another assignment of such Bidder.

15. Code of integrity

No official of a procuring entity or a bidder shall act in contravention of the codes which includes

A. Prohibition of:

i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.

ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained or an obligation avoided.

iii. any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process.

iv. improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.

v. any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract; which can affect the decision of the procuring entity directly or indirectly.

vi. any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.

vii. obstruction of any investigation or auditing of a procurement process.

viii. making false declaration or providing false information for participation in a tender process or to secure a contract;

B. Disclosure of conflict of interest.

Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a)

with any government entity in India during the last three years or of being debarred by any other government procuring entity.

In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, concludes that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, the Bidder's proposal will be summarily rejected.

16. Fraud and Corruption

The Bidders is required to observe the highest standard of ethics during the procurement and execution of such contracts. In pursuance of this policy, the following shall apply:

a) For the purpose of this provision, the terms are defined and are set forth as follows:
   i. **"Corrupt Practice"** means behaviour on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves and/or those close to them, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the Contract of any such official in the procurement process or in Contract execution.
   ii. **"Fraudulent Practice"** means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract to the detriment of the borrower, and includes collusive practices among bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the borrower of the benefits of free and open competition

b) NETF will reject Proposal for award if it determines that the bidder recommended for awardhas engaged in corrupt or fraudulent practices in competing for the Contract.

c) NETF will declare a Company ineligible either indefinitely or for a stated period of time, to be awarded a Contract if it, at any time, determines that the Company has engaged in corrupt or fraudulent practices in competing for, or in executing, and the assignments awarded by NETF.

17. Compliant Proposals / Completeness of Response

I. Bidder is advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

II. Failure to comply with the requirements of this paragraph may render the Proposal non- compliant and non-responsive and the Proposal may be rejected.

III. Bidders must:
   i. Include all documentation specified in this RFP;
   ii. Follow the format of this RFP and respond to each element in the order as set out in this RFP

18. Sub-contracting

Sub-contracting is not allowed in this bid.

19. Queries / Clarifications on the RFP

Queries / Request for clarifications on the RFP shall be sent by Bidders through email only in the format

specified in the RFP not later than the date and time specified in the 'Bidding Schedule'. All the requests shall be addressed to NETF contact person assigned as mentioned in the 'Bidding Schedule'. No request for clarification from any Bidder shall be entertained after the last date and time mentioned in the 'Bidding Schedule'.

20. Supplementary Information/Corrigendum/Amendment to the RFP

I. At any time prior to the deadline (or as extended by NETF) for submission of bids, NETF for any reason, whether at its own initiative or in response to clarifications requested by the Bidder may modify the RFP document by issuing amendment(s) or issue additional data to clarify an interpretation of the provisions of this RFP.

II. Such supplements / corrigendum to the RFP issued by NETF would be displayed on the e- Tendering Portal / Website of NETF and may additionally also be communicated by e-mail to the Bidders.

III. Any such supplement / corrigendum / amendment shall be deemed to be incorporated by this reference into this RFP.

IV. Any such supplement / corrigendum / amendment will be binding on all the Bidders.

V. NETF will not be responsible for any misinterpretation of the provisions of this Tender document on account of the Bidders failure to update the Bid documents based on changes announced through the website.

VI. In order to allow Bidders a reasonable time to take the supplement / corrigendum / amendment(s) into account in preparing their bids, NETF, at its discretion, may extend the deadline for the submission of bids.

21. Proposal Preparation Costs

The Bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of Proposal, in providing any additional information required by NETF to facilitate the evaluation process, and in negotiating a definitive service Agreement all such activities related to the Bid process. This RFP does not commit NETF to award a Contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award of the Contract for implementation of the Project.

22. Right to terminate the process

NETF makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. Further, this RFP does not constitute an offer by NETF. The RFP does not commit NETF to enter into a binding Agreement in respect of the Project with the Bidders.

23. Modification, Substitution or Withdrawal of Proposals

No Proposal may be withdrawn in the interval between the deadline for submission of Proposals and the expiration of the validity period specified by NETF. Entire Bid Security may be forfeited if any of the Bidders withdraw their Bid during the validity period.

24. Language of Bids

This bid should be submitted in English language only.

25. Ownership of Application / Documents Prepared by the Successful Bidder

All plans, specifications, designs, reports, other documents, patent and software including the all the hardware shall be absolute property of NETF. The Successful Bidder shall transfer to NETF all Intellectual Property rights. The Successful Bidder shall not use anywhere, without taking permission, in writing, from the NETF and NETF reserves right to grant or deny any such request.

26. Confidentiality

a) The Bidder shall not use Confidential Information, the name or the logo of NETF and NETF except for the purposes of providing the Service as specified under this Contract;

b) The Bidder may only disclose Confidential Information in the following circumstances:
   i. with the prior written consent of NETF;
   ii. to a member of the Bidder's Team ("Authorized Person") if:
      - the Authorized Person needs the Confidential Information for the performance of obligations under this Contract.
      - the Authorized Person is aware of the confidentiality of the Confidential Information and is obliged to use it only for the performance of obligations under this Contract. The Bidder shall do everything reasonably possible to preserve the confidentiality of the Confidential Information to the satisfaction of NETF.

c) The Bidder shall notify NETF promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of NETF.

d) The Bidder shall be liable to fully recompense NETF for any loss of revenue arising from breach of confidentiality. NETF reserves the right to adopt legal proceedings, civil or criminal, against the Bidder in relation to a dispute arising out of breach of obligation by the Bidder under this clause.

27. Evaluation Process

NETF shall evaluate the responses of the bidders to this RFP and scrutinize the supporting documents /documentary evidence. Inability to submit the requisite supporting documents / documentary evidence by the bidders, may lead to rejection. The decision of NETF in the evaluation of proposals shall be final. No correspondence will be entertained outside the processof evaluation with NETF. NETF may ask for meetings with the Bidders or may issue in writing/email to seek clarifications or conformations on their proposals. During the Proposal Evaluation, NETF reserves the right to reject any or all the proposals. Each of the Proposals shall be evaluated as per the criteria and requirements specified in this RFP. The Evaluation Committee (EC) constituted by the NETF shall evaluate the responses to the RFP and all supporting documents & documentary evidence as mentioned in this section of the RFP. NETF reserves the right to check/ validate the authenticity of the information provided in the Pre- qualification criteria and Financial Evaluation and the requisite support must be provided bythe Bidder.

The bid evaluation will be carried out in a three-stage process as under:

A. Pre-Qualification/Eligibility Evaluation

a) Evaluation of Technical bid

b) Evaluation of Financial bid

Pre-Qualification/Eligibility Evaluation

I. The evaluation of the bidders will be carried out by the Committee as per the pre- qualification / eligibility criteria defined in the tender document. Only the bidders who fulfil the given pre-qualification / eligibility Criteria shall be eligible for next round of evaluation i.e. Technical evaluation. Nonconforming bids will be rejected and will not be eligible for any -responsive. further processing.

II. The bidder can be a CSP or an authorized partner of the CSP. In case of an authorized partner, the CSP can authorize any number of bidders for the purpose of this RFP.

III. Each bidder (in case of authorized partner of any CSP) shall be allowed to submit the bid with one CSP only.

IV. The eligibility criteria in case the bidder is a CSP empanelled with MeitY or an authorized partner of a CSP empanelled with MeitY is as per Annexure H.

V. Notwithstanding anything stated above, the Consignee reserves the right to assess bidder's capability and capacity to perform the contract, should circumstances warrant such an assessment in the overall interest of the NETF or project.

VI. Technical bids will also be reviewed for compliance with the necessary instructions, terms and conditions, scope of work, formats etc. as outlined in this tender.

VII. NETF reserves the right to physically verify the office or any document provided by the bidder in the way NETF desires.

a) Evaluation of Technical bid

I. The evaluation of the bidders will be carried out by the Committee as per the Technical Evaluation criteria defined in the RFP document. Only the bidders who qualify in the technical evaluation round shall be eligible for next round of evaluation i.e. Financial/Financial Bid Opening. Bids of the bidders, who do not qualify in thetechnical evaluations stage, will be rejected and will not be eligible for any further processing.

II. The technical evaluation of the bidders shall be done as per Annexure J.

III. Only those bidders who secure a Technical Score of 80% (i.e. minimum 160 out of 200) or more shall be considered for evaluation of their Financial bid.

b) Phase II - Evaluation of Financial bids:

I. Financial bids would be opened only for those Bidders, who secure the qualifying marks in the Technical Evaluation as explained above, on the prescribed date in the presence of bidder's representatives.

II. It is mandatory for bidder to quote discount percentage on the CSP List pricing

for the CSP services and prices for the services mentioned in financial bid Part B.

III. **The financial evaluation of the bidders will be only on value of "discount percentage" on the CSP list pricing as per Financial bid Part A.**

IV. It is mandatory that the list price of CSP Services mentioned in the Technical compliance (Annexure L) should be available on the CSP website. The process to get the price from the CSP website (price calculator) should be explained during the presentation by the bidder.

V. NETF will empanel the CSPs (in case the bidder is CSP) or only one authorized partner of each CSP. The bidders with highest discount percentage (H1) as per Financial Bid Part A on the CSP List price of the CSP services mentioned in the Technical compliance (Annexure L) shall be eligible for empanelment. In case the discount percentage comes out to be same for two or more bidders, then the bidder having higher technical score will get empanelled. The prices mentioned by the H1 Authorized Partner of all CSPs or the CSPs (in case the service provider is CSP) will be discussed with the H1 bidder to optimize the quoted value of "discount percentage" on the CSP list pricing as per Financial bid Part A to inline this prices as per the market by a duly constituted Rate Reasonability Committee, the decision of which would be final and binding on the successful bidders.

VI. The prices mentioned by all the H1 Authorized Partner of all CSPs or the CSPs (in case theservice provider is CSP) will be discussed with all the H1 bidders to optimize the quoted rates of each of the line items on lower side to inline the prices as per the market for all theservices mentioned in Part B of financial Sheet by a duly constituted Rate Reasonability Committee, the decision of which would be final and binding on the successful bidders.

VII. In case of an abnormally High percentage and low other service prices, i.e. one in which the bid price, in combination with other elements of the bid, appears so low that it raises material concerns as to the capability of the bidder to perform the contract at the offered price. NETF may in such cases seek written clarifications from the bidder or CSP including detailed price analyses of its bid price in relation to scope, schedule, allocation of risks and responsibilities and any other requirements of the bid document. If, after evaluating the price analyses, NETF determines that the bidder has substantially failed to demonstrate its capability to deliver the contract at the offered price, NETF may reject the Bid/Proposal. This applies for financial bid submitted at the time of bid response to be submitted as per the RFP.

VIII. The empanelment of the service providers only for the categories mentioned in Technical Compliance (Annexure L and Annexure M)

IX. Failure to abide the RFP conditions may result into forfeiture of EMD & PBG.

X. Any conditional financial bid will lead to disqualification of the entire bid and forfeitureof the EMD.

XI. Bidder quoting negative discount percentage or rates will be treated as non-

responsive andwill result in forfeiture of the EMD.

XII. Financial bid will be inspected to ensure conformance to the format provided in the tenderdocument.

XIII. If there is any discrepancy between words and figures in any part of the financial bid, the amount indicated in words will prevail.

XIV. The bidder shall quote the discount percentage and prices as per the price format given in the Part A and Part B - FInancial Bid of this RFP.

28. Notification of Award of Contract

I. Acceptance from all the H1 Authorized Partner of all CSPs or the CSPs (in case the serviceprovider is CSP) to optimize the quoted rates of each of the line items on lower side to inline the prices as per the market for all the services mentioned in Part B of Financial Sheet.

II. The notification of award will constitute the formation of the empanelment contract.

29. Prices

The discount percentage and prices quoted in the Financial bid shall be inclusive of all statutory duties & taxes except GST. Only GST charged in the invoice will be paid other than that no other taxes/duties/levies will be paid.

30. Additional Services

In case NETF determines that there are additional services that are being sought by the Clients, NETF may request all the "Empanelled Service Providers" to submit the prices for such additional services at any time during the validity of the contract on same terms and conditions. The rates shall be submitted as per price format provided by NETF. No conditional bid would be accepted and the price format should be strictly adhered to. The sealed bids would be opened in the presence of the representatives of the Empanelled bidders who may wish to be present.

31. Payment Terms

I. Payment to the Supplier shall be made in Indian Rupees through account payee cheque / NEFT / RTGS, Payments will be done only on the back-to-back basis on receipt of the related payment/funds from the end client, subject to acceptance of the deliverables from the end client as per the submission of the required document.

II. The invoices shall be raised only using GST No. of NETF.

III. The invoices must be based on work orders (or any amendments thereof) issued by the NETF.

IV. The invoices must be based on resources actually consumed and committed.

V. The invoices should be separately generated for each work order for the

particular payment period.

VI. NETF and NETF end client may request for below documents (if required):
   i. Detailed usage report (Utilization Report) providing details of the consumption of theindividual services during the payment period
   ii. SLA measurement report

VII. The client should provide the SLA breaches (if any) to deduct the payment against the workorder.

VIII. Payments shall be subject to deductions / damages / penalties of any amount for which the Supplier is liable under the contract. Further, all payments shall be made subject to deduction of TDS (Tax Deduction at Source) at the rate applicable from time to time as per the Income-Tax Act, 1961 and any other applicable deductions/ taxes.

32. NETF Contract finalization and Award

The NETF shall reserve the right to negotiate with the Bidder(s) whose Proposal has been ranked best value bid on the basis of Technical and Financial Evaluation to the proposed Project, as per the guidance provided by Central Vigilance Commission (CVC). On this basis the draft Contract agreement would be finalized for award & signing. Subsequent to receipt of valid Performance Guarantee from the successful Bidder, the parties shall enter into, incorporating all clauses, pre-bid clarifications and the Proposal of the Bidder, between the NETF and the successful Bidder. In case of exigency/ non-performance / default, if NETF gets the work done from elsewhere, the difference in the cost of getting the work done will be borne by the successful Bidder.

33. Contract Period:

The contract signed with "Empanelled Service Provider" shall be for a period of three years from the date of its execution, and can be renewed as per relevant clause for a further period of one year on same terms and conditions. NETF reserves the right to curtail or extend the validity of contract based on performance as per SLA.

34. Performance Bank Guarantee

I. On receipt of a letter of intent from the NETF, the successful Bidder will furnish a Performance Bank Guarantee equivalent to 10% per cent of the total Contract value, on or before the signing of the subsequent Contract, within 15 days from notification of award. In case the successful Bidder fails to submit Performance Bank Guarantee within the time stipulated, the NETF may at its sole discretion cancel the letter of intent without giving any notice and encase the EMD furnished by the Bidder, in addition to any other right available to it under this RFP.

II. The Performance Bank Guarantee furnished by the successful Bidder shall be as prescribed in SLA. The successful Bidder shall ensure, the Performance Guarantee is valid at all times during the Term of the subsequent Contract (including any renewal) and for a period of 60 days beyond all Contractual obligations, including warranty terms.

III. Performance Bank Guarantee will have to be renewed for such further periods till validity of the Contract and thereafter the Performance Bank Guarantee shall be refunded to the vendor without any interest.

IV. The vendor should not assign or sublet any activity under the Contract or any part of it to any other agency. Failure to do so shall result in termination of Contract and forfeiture of Performance Bank Guarantee

V. NETF may, at any time, terminate the Contract by giving written notice to the vendor without any compensation, if the vendor becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to NETF.

VI. In the event the selected bidder's company or the concerned division of the company is taken over / bought over by another company, all the obligations and execution responsibilities under the agreement with NETF, should be passed on for compliance by the new company in the negotiation for their transfer.

35. Failure to Agree with the Terms and Conditions of the RFP

VII. Failure of the successful Bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event NETF may award the Contract to the next best value Bidder or call for new proposals from the interested Bidders.

VIII. In such a case, the NETF shall invoke the PBG of the most responsive Bidder.

36. Performance Measurements

IX. Unless specified by NETF to the contrary, the Bidder shall perform the Services and carry out the scope of work in accordance with the terms of this Contract, Scope of Work, Service Specifications and Service Levels as laid down in this tender.

X. If the Contract, Scope of Work, Service Specification includes more than one document, then unless NETF specifies to the contrary, the latter in time shall prevail over a document of earlier date to the extent of any

inconsistency.

XI. NETF reserves the right to amend any of the terms and conditions in relation to the Contract / Service Specifications upon agreement with the System Integrator/service provider and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfillment of the Schedule of Requirements.

XII. If any such change causes an increase or decrease in the cost of, or the time required for the Bidder's performance of any part of the work under the Contract, whether changed or not changed by the order, an equitable adjustment shall be made in the Contract Value or time schedule, or both, and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause must be asserted within thirty (30) days from the date of the Bidder's receipt of NETF's changed order.

37. Resolution of dispute amicably/through arbitration

The law of the land shall govern this contract. Any dispute between the parties arising in connection with the performance of this contract shall be resolved amicably between the representatives nominated by both the parties through the process of negotiation. In case the dispute is not resolved, then it shall be referred to the Chairman, NETF and the Chief of the opposite party for settlement.

If the dispute is not resolved, then it shall be referred to the Sole Arbitrator for arbitration proceedings as per the provisions contained in the Indian Arbitration and Conciliation Act, 1996(as amended from time to time and in force at the time when the reference is made). The Sole Arbitrator shall be appointed with the consent of both the parties. The Sole Arbitrator shall be appointed within a period of 60 days from date of receipt of written notice/demand of appointment of arbitrator from either party. The seat and jurisdiction of the arbitration proceedings shall be at New Delhi. The arbitration proceedings shall be in English language. The cost of the arbitration proceedings shall be borne equally by both the parties as per Arbitration rules.

If any dispute remains still unsettled, in that case, the same shall be adjudicated by the Courts of Law at New Delhi.

38. Work Order

I. The work order will be issued to the empanelled service provider after deducting discount percentage from the CSP list prices (In INR) on that day (on the day of issuing work order) with the addition of prices for the other services as mentioned in Financial bid.

II. Whenever the Client needs the Cloud service, the work order can be issued in two ways:
   a) If any client wants any specific services from a particular CSP, then the work order will be issued to H1 bidder of that CSP directly or directly to CSP (In case the bidder is CSP).
   b) If client provides only the requirement containing a list of line items (as identified in Technical Compliance and Financial Bid). For each requirement, the discount percentage and prices quoted for the complete set of line items contained in the requirement by H1 service providers will be taken to decide L1 bidder. If for any item in the requirement, the "Empanelled Service Provider" has not quoted rates, such bidderwill not be considered for L1 purpose.

III. For Lift-and-Shift workloads, client transforms their requirements to cloud based requirements (e.g., right-size instance, right-size storage, right storage class, standard instance size, application services, native security services) based on the utilization, storage use cases and defines its comprehensive cloud requirements (e.g., compute, storage,networking, security, monitoring services).

IV. Client will provide the indicative & maximum consumption of cloud services (as per the list of line items identified in the Financial bid) during the contract duration to prepare the bill of material and evaluation will be carried out on the Total Cost of Ownership (or whole-life-cost of the contract). Client may retain the agility to scale-up or scale-down by also including lower and higher configuration instances in the bill of material prepared forevaluation.

V. Indicative Guidelines: For lift-and-shift workload migrations, client should consider thecurrent utilizations and start small and scale up/down as per the requirements.
   a) Right Size instances and start with smaller instances based on the current utilizations
   b) Start with fewer instances and avail Auto-scaling Feature; don't start with peak load
   c) Identify the pre-production environments and use scheduling to shut-down whenenvironment is not required to be running – use on-demand pricing
   d) Right size storage and start with smaller storage capacity based on the utilizations
   e) Use the appropriate storage service based on the storage use case– SSD, HDD, File, Object Storage, and Archival
   f) Leverage fully-managed services (e.g., DNS Service, Load Balancer) where there's norequirement for additional Virtual Machines

VI. An example of how L1 would be decided: Suppose, the Client needs a "Windows VM – 1vCPU, 2 GB RAM" with 100 GB of "Premium Block Storage". For this requirement or item(s), the total cost of each of the "Empanelled Service Provider" will be calculated based onthe prices identified in the Financial bid. The "Empanelled Service Provider" offering lowest prices for the Client's requirement would be termed as L1 (Least Cost) bidder for that particular requirement. Similarly, L1 would be identified for each subsequent requirement

of the Client. In case the cost for a particular requirement comes out to be same for two or more "Empanelled Service Provider", then the firm having higher Technical Score will be declared as the L1 bidder / Supplier for that particular requirement.

VII. For a particular requirement, work order will be placed to only the L1 bidder, who, after submission of Performance Securities, would be known as the Supplier for that particular requirement. In case L1 bidder denies or is unable to fulfil the requirement, NETF reservesthe right to obtain the services from the next lowest bidder.

VIII. Failure to provide services as per requirement by bidder may result into forfeiture of EMD, PBG & termination of the contract.

IX. The NETF reserves the right to place a work order of any time duration.

X. For large scale project or for extra educational discount, CSP can offer the Extra discount (over the discount price quoted by H1 bidder) thorough it's authorize partner to NETF onwork orders.

XI. NETF will intimate the Supplier in writing regarding any extension in the work order. Extension in the contract would not lead to extension of any of the in-force work orders.

XII. The contract between Client and NETF will adopt the following cloud aligned principles

a) Retain operational agility to scale up / scale down resources; add / remove services; within the maximum value of the contract.

b) The maximum contract value is not any commitment by the client. Client will only payfor the resources that are consumed or committed (e.g., reserve instances) in that payment period and the payments may vary from one payment period to the other basedon the consumption.

c) A prior intimation through mail or letter by Client shall be provided to NETF wheneverscale-down or scale-up (including auto scaling) of resources and add or remove of services takes place.

XIII. Contract termination shall automatically lead to termination or expiry of all work orderswhich were issued based on the contract.

XIV. The supplier must complete the obligation of the work order as per the signed contractuntil the time duration which will be mention in the work order.

39. Escalation Matrix

The "Empanelled Service Providers" / Supplier(s) should provide at-least 3 level escalation matrix for providing resolution of the complaints at local level.

40. Annexures

Annexure A – Declaration Sheet format

<< Organization Letter Head >>

DECLARATION SHEET

We,_____hereby certify that all the information and data furnished by our organization with regard to this tender specification are true and complete to the best of our knowledge. I have gone through the specification, conditions and stipulations in details and agree to comply with the requirements and intent of specification.

We further certified that our organization meets all the conditions of eligibility criteria laid down in this tender document. Moreover, we will support on regular basis with technology / product updates and extend support for the warranty.

Name Bidding Company/Vendor/ Manufacturer/ Agent	
Address	
Incorporation status of the firm (public limited / private limited, etc.)	
Date of registration	
Phone	
Contact Person Name with (Email-Id and Contact number)	
GST Number	
PAN Number	
DD Bank Name and No (For EMD)	
Please mention that the bidder is CSP **or** Authorized Partner of CSP	
Name of CSP (If Bidder is Authorized Partner of CSP)	
Kindly provide bank details of the bidder in the following format: a) Name of the Bank	
b) Account Number	
c) IFSC Code	
d) Kindly attach scanned copy of cancelled Cheque book page to enable us to return the EMD to unsuccessful bidder	

Name:_____

Signature and Seal of the Bidder

Annexure B – Letter of Undertaking

LETTER OF UNDERTAKING

(ON THE LETTER HEAD OF THE BIDDER)

To
Chairman,
NETF, New Delhi 110070

Sir,

SUBJECT- Letter of undertaking

This bears reference to NETF Bid No._____Dated_____We, hereby, accept all the terms and conditions for submitting bid as mentioned in this Bid Document.

We hereby certify that no terms and conditions have been stipulated by us in the Financial Bid.

We warrant that the services do not violate or infringe upon any patent, copyright, trade secret or other property right of any other person or other entity. We agree that we shall not prevent NETF from any claim or demand, action or proceeding, directly or indirectly resulting from or arising outof any breach or alleged breach of any of the terms & conditions of bid document and contract.

The above document is executed on..... at (place)_____and we accept that if anything out of the information provided by us is found wrong, our bid/ work order shall be liable for rejection.

Thanking you,

Yours faithfully,

Name:_____

Signature and Seal of the Bidder

Date:

Place:

Annexure C – Power Of Attorney

Know all men by these presents, we ..... (name of firm and address of the registered office) do hereby constitute, nominate appoint and authorize Mr./Ms……..son/daughter/wife of …….. and presently residing at……., who is presently employed with /retained by us and holding position of as our true and lawful attorney (hereinafter referred to as the "Authorized Representative") to do in our name and on our behalf, all such acts, deeds and things are as necessary or required in connection with or incidental to submission of our proposal for and selection as the <project title> for the <name of the client>… project, proposed to be developed by the…….. (the "client") including but not limited to signing and submission of allapplications, proposals and other documents and writings, participating in pre bid and other conferences and providing information /responses to the client, representing us in all matters beforethe Client, signing and execution of all contracts and undertakings consequent to acceptance of ourproposal and generally dealing with the client in all matter in connection with or relating to or arising out of our Proposal for the said project /or upon award thereof to us till the entering into ofthe Agreement with the client.

AND, we do hereby agree to ratify and confirm all acts, deeds and things lawful done or caused tobe done by our said Authorized Representative pursuant to and in exercise of the powers conferredby this power and Attorney and that all acts, and things done by our said Authorized Representativein exercise of the powers hereby conferred shall and shall always be deemed to have been done byus.

[IN WITNESS WHEREOF WE……THE ABOVE NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON

THIS …….. DAY OF..... 2021.

For .....(Name and registered address of client)

(Signature, name, designation, and address)

Witness

1. (Signature, name and address)

2. (Signature, name and address)

Notarized

Accepted

…….

(Signature, name, designation, and address of the attorney)

Notes:

1. The mode of the execution of the power of Attorney shall be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executants (s) and when it is so required the same should be under seal affixed in accordance with the required procedure.
2. Wherever required, the applicant should submit for verification the extract of the charter documents and other documents such as a resolution/Power of Attorney in favor of the person executing this Power of Attorney for delegation of power hereunder on behalf of theapplicant.
3. For a Power of Attorney executed and issued overseas, the document will also have to be legalized by the Indian Embassy and notarized in the jurisdiction where the Power and Attorney is being issued. However, the Power of Attorney provided by the applicants from countries that have signed The Hague Legislation Convention, 1961 are not required to be legalized by the Indian Embassy it is carries a conforming Apostle certificate.

Annexure D - Performa For Declaration from bank on Proceedings UnderInsolvency And Bankruptcy Code, 2016

Tender No.:……..

Name of Work:……..
Bidder ’s Name : ..... .

I/ We, M/s._____declare that:-

a) I /We am / are not undergoing insolvency resolution Process or liquidation or bankruptcy proceeding as on date.
b) I /We am / are undergoing insolvency resolution process or liquidation or bankruptcy proceeding as on date as per Details mentioned below. (Attached detail with technical bid)

Note: Strike out one of above which is not applicable.

It is understood that if this declaration is found to be false, NETF shall have the right to reject my / our bid, and forfeit the EMD, if the bid has resulted in a contract, the contractwill be liable for termination without prejudice to any other right or remedy (including holidaylisting) available to NETF.

Place:
Date:

Signature of Bidder

Name of Signatory

Signature of the authorized bank Official

Name of the Bank

Seal of the bank

Annexure E - Undertaking For Non-Blacklisting

This is to confirm that we M/s_____(give full address) have not been declared neither **failed to perform on any Agreement, nor have been expelled from any project or Agreement nor any Agreement terminated** for breach by the us (Agency) in any of the government department and public sector undertaking /enterprise or by any other Client in India, in last five year before release of advertisement.

If the above information found false at any stage after the placement of Work Order / Agreement, NETF will have full right to cancel the Contactand forfeit the Performance Guarantee. All the direct and indirect cost related to the cancellation ofthe order will be borne by us besides any legal action by NETF which shall be deemed fit at that point of time.

Authorized Signatory

Note: *The undertaking regarding the non-blacklisting of firm is to be submitted on a non-judicial stamp paper of Rs. 100/- (Rupees Hundred only).*

Annexure F - Technical Bid Submission Letter

To:

Chairman

NETF, New Delhi 110070

Subject: Submission of the Technical bid for Empanelment of MeitY Empanelled CSPs ortheir Authorized Partner for offering Cloud Services

Dated:____/___/2023

Dear Sir,

We, the undersigned, offer to provide cloud services to NETF and NETF's end Client.

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

We undertake, if our Proposal is accepted, to initiate the services related to the assignment notlater than the date indicated in the contract agreement.

We agree to abide by all the terms and conditions of the RFP document. We would hold theterms of our bid valid for 180 days as stipulated in the RFP document.

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:

In the capacity of:

Address:

E-mail:

Annexure G - Eligibility Criteria

The compliance against each of the particulars provided under Clause 6.13.1.IV (irrespective of whether the bidder is a CSP empanelled with MeitY or its authorized partner) is to be submitted asper below format:

S. No.	PQ criteria	Documents Required	Supporting Document	Page No./File Name	Compliance (Yes/No)
1.	The bidder must submit Declaration Sheet	Authorization Certificate from as per Annexure A			
2.	The bidder must submit Letterof undertaking	Authorization Certificate from as per Annexure B			
3.	The bidder should have valid GST and PAN number.	Self-attested copy of the GST certificate and PAN card.			
4.	The bidder should be either: I. A company registered under the Indian Companies Act, 2013 OR II. A partnership firm registered under the Limited Liability Partnerships (LLP) Act, 2008 OR III. A partnership firm registered under the Indian Partnership Act, 1932.	a. Certificate of Incorporation/ Certificate of Registration b. Memorandum and Articles of Association/ Partnership deed.			
5.	The bidder must submit Powerof Attorney	Authorization Certificate from as perAnnexure C			
6.	The bidder must ensure to deposit EMD OR The bidder must ensure to submit NSIC/MSME certificate	Submission of DD/ OR Submission of MSME Certificate and Performa For			

		Declaration from bank on Proceedings Under Insolvency And Bankruptcy Code, 2016 as per Annexure D and financial solvency certificate of issued not earlier than 3 months from the last date of bid submission			
7.	Bidder should not be blacklisted by any state government, Central Government/State Government/PSU/Government Bodies/Autonomous Bodies/Private Sector or court of law in the last 5 years.	The bidder shallfurnish an undertaking duly attested by notary in a non-judicial stamp paper of value INR 100/- (Rupees One Hundred Only) as per Annexure E.			
8.	Technical Bid Submission Letter	Self-Certified copy of Annexure F			
9.	The bidder or the CSP of which the bidder is an authorized partner should be empanelled with MeitY for providing cloud services.	Self-certified copy of MeitY, GoI empanelment as CSP.			
10.	If the bidder is an authorized partner of a CSP empanelled with MeitY, the eligibility criteria shall provide an Authorization Certificate from a MeitY empanelled CSP which states clearly that the bidder has been authorized to participate in this bid.	Authorization Certificate from as per Annexure H			

11.	The Bidder (in case bidder is the CSP) or the CSP of which the bidder is an authorized partner should have minimum Average Annual turnover of at least Rs. 400 Cr from Cloud Services for last three financial years i.e., 2019-20, 2020-21 & 2021-22.	A certificate from Statutory Auditor/Chartered Accountant clearly specifying the turnover during the last threefinancial years as per Annexure J Part A (i.e. 2019-20, 2020-21 & 2021-22).			
12.	The Bidder (in case bidder is the authorize partner of CSP) should have minimum Average Annual turnover of at least Rs. 50 Cr for last three financial years i.e., 2019-20, 2020-21 & 2021-22.	A certificate fromStatutory Auditor/Chartered Accountant clearlyspecifying the turnoveralong with net worth andprofit during the last threefinancial years as perAnnexure I Part B (i.e.2019-20, 2020-21 & 2021-22).			
13.	The Bidder (in case bidder is the authorize partner of CSP) should have positive net worth for last three financial years i.e., 2019-20, 2020-21 & 2021-22.	A certificate fromStatutory Auditor/Chartered Accountant clearlyspecifying the turnoveralong with net worth andprofit during the last threefinancial years as perAnnexure I Part B (i.e 2019-20, 2020-21 & 2021-22).			
14.	The bidder should be ISO 9001:2015 certified and ISO 27001:2013	Self-certified copy of certification which is valid on date of bid submission.			

Note: All the above mentioned documents have to be scanned and uploaded.

Name:_____

Signature and Seal of the Bidder

Annexure H - MeitY empanelled CSP Authorization Form

No._____dated_____

To

_____

_____

Dear Sir:

Bid No. _____

CSP <<NAME OF THE CSP>> (hereafter "CSP") is pleased to support <<PARTNER NAME>>for the pursuit of the Tender for <<TENDER REFERENCE NUMBER>>.

I/We confirm that as on the date of this letter <<PARTNER NAME AND ADDRESS is authorized by CSP to use our cloud services for the purposes of the above referenced tender.Should <<PARTNER>> be awarded the contract resultant from the above referenced tender,CSP will support <<PARTNER>> with our commercially available cloud services in accordance with the prevailing commercial terms and agreements.

Yours faithfully,

(Name and signature of Authorized Person):_____

(Name of MeitY empanelled CSP):_____

Note: This letter of authority should be on the letterhead of the manufacturer or OEM and shouldbe signed by a person competent and having the power of attorney to legally bind the manufacturer

Annexure I - Annual Turn Over From

Part A

Name of the Organization:

Sl. No.	Financial Year	Annual Turnover From Cloud Service
1.	2019-20	
2.	2020-21	
3.	2021-22	
Total		
Total in Words		
Average		
Average in Words		

Note:

- Values entered in words will be treated as final.

Signature with Seal of the Chartered Accountant

Name of Chartered Accountant

Signature of Authorize person with Seal of the Bidder

Part B

Name of the Organization:

Sl. No.	Financial Year	Annual Turnover (In Rs.)	Net Worth (In Rs.)
1.	2019-20		
2.	2020-21		
3.	2021-22		
Total			
Total in Words			
Average			
Average in Words			

Note:

- Certificate from Statutory Auditor certifying Balance sheet and P&L statement only for all three years to be attached with signature and seal of chartered accountant.
- Values entered in words will be treated as final.

Signature with Seal of the Chartered Accountant

Name of Chartered Accountant

Signature of Authorize person with Seal of the Bidder

Annexure J - Technical Evaluation Criteria:

The compliance against the particulars mentioned from Sl. No. 1 to 6 of Clause 6.13.2.II Part A isto be submitted as per below format: -

S.No.	Evaluation Criteria	Maximum Marks Weightage	Documentary Evidence to be submitted	Supporting Document	Page no./File name
1.	The Bidder (in case bidder is the CSP) or the CSP of which the bidder is an authorized partner have Average Annual turnover from cloud services for last three financial years i.e., 2019-20, 2020-21 & 2021-22 • >=400 Cr and <1000 Cr.:5 marks • >=1000 Cr and <2000 Cr.: 10 Marks • >=2000 Cr: 20 Marks	20	A certificate from Statutory Auditor/Chartered Accountant clearly specifying the turnover along with net worth and profit during the last threefinancial years as per Annexure I Part A (i.e2019-20, 2020-21 & 2021-22).		
2.	The Bidder have Average Annual turnover for last three financialyears i.e., 2019-20, 2020-21 & 2021-22. • >=50 Cr and<75 Cr.: 2 Marks • >=75 Cr and<100 Cr.: 5 Marks • >=100 Cr: 10 Marks	10	A certificate from Statutory Auditor/Chartered Accountant clearly specifying the turnoveralong with net worth andprofit during the last threefinancial years as perAnnexure I Part B (i.e2019-20, 2020-21 & 2021-22).		
3.	The Bidder have Average Annual net worth for last	10	A certificate from Statutory Auditor/Chartered		

	three financial years i.e., 2019-20, 2020-21 & 2021-22 . • >=5 Cr and<10 Cr.: 2 Marks • >=10 Cr and<20 Cr.: 5 Marks >=20 Cr: 10 Marks		Accountant clearly specifying the turnover along with net worth and profit during the last three financial years as per Annexure I Part B (i.e. 2019-20, 2020-21 & 2021-22).		
4.	The Bidder should have Cloud Service Projects of Central Government/ State Government/ PSUs in the last three financial years. (i.e., from 01.04.2019 to the bid submission date) • 0 Projects: No Marks • >=0 projects and <3 projects.: 2 Marks • >=3 projects and <7 projects.: 5 Marks • >=7 projects: 10 Marks	10	Work Orders containing relevant details as desired for evaluation		

5.	The Bidder should have Cloud Service Project of more than 1 Cr project value in last 3 years (i.e., from 01.04.2019 to the bid submission date) from a single project: • 0 Projects: No Marks • >=1 project: 2 Marks • >=2 projects: 5 Marks • >=3 projects: 10 Marks	10	Work Orders containing relevant details as desired for evaluation		
6.	The Bidder should have Cloud service Projects from State or Centre Govt. university or from any Institutions of National Importance in the last three financial years. (i.e., from 01.04.2019 to the bid submission date) • 0 Projects: No Marks • >=1 project: 2 Marks • >=2 projects: 5 Marks • >=3 projects: 10 Marks	10	Work Orders containing relevant details as desired for evaluation		

7.	Number of Data Centers in India from where the MeitY empaneled Cloud Services are offered (The data centers should be in distinct physical locations) • One location – 0 marks • Two locations –5 marks • Three locations or more – 10 marks	10	Self-certified copy from CSP for different data centres as per Annexure K.		
9.	SOC Certifications for Cloud services offered by the CSPs: • Not certified for SOC1, SOC2, and SOC3: 0 marks • Certified for any one of SOC1, SOC2, andSOC3: 2 mark • Certified for any two of SOC1, SOC2, and SOC3: 5 marks • Certified for SOC1, SOC2, and SOC3: 10 marks	10	Bidder should provide the report for the SOC certification. Also, the bidder (CSP) will provide the URL for the SOC Report.		

10.	The Bidder (in case of CSP) or CSP of which the bidder is an authorized partner should be in leader's quadrant for Cloud Infrastructure as a Service, Worldwide as per latest Gartner Report.	10	Documentary evidence for the same should be provided.		
11.	Technical Compliance • 2 Marks each for Basic CSP Services as per Annexure L • 3 Marks each for Advance Services of CSP as per Annexure L • 2 Marks for other Cloud related services as per Annexure M	60	As per Annexure N and Annexure M		
12.	Technical presentation 5 Marks – Revenue Generation Model with NETF 10 Marks – Go-To Market Strategy along with NETF Team 10 Marks – Works in Education Sector in past 3 year 5 – Capability of the bidder and CSP 10 Marks – Company Strength in Pan India and International client	40	Time, Date and place will be informed later.		

Note: All the above-mentioned documents have to be scanned and uploaded.

Signature with Seal of the Bidder

Annexure K – Data Centre Location Certificate

To Dated:___/____/2023

Chairman
NETF, New Delhi-110070

Subject: Submission of the Technical Compliance for location of CSP data centerDear

Sir,

I/We am/are the Cloud Service Provider, we have_____no. of different data centers in India which are located in different physical locations.

Signature of the CSP

Signature with Seal of the Bidder

Annexure L – Technical Compliance for CSP Services

To

Dated:___/____/2023

Chairman
NETF, New Delhi-110070

Subject: Submission of the Technical Compliance of CSP servicesDear

Sir,

I/We am/are the Cloud Service Provider and all of our offered Cloud Service Offerings areas below is available in India Data Centers:

Basic Service:

S. No.	Service Category	Minimum Requirement for compliance	Compliance Yes/ No	Service Names and URL of the services for description	CSP Website Pricing URL of the Service
1.	Compute	• Must support variety of operating systems including: Linux, Ubuntu, Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, openSUSE Leap, Fedora, Fedora CoreOS, Debian, CentOS, Gentoo Linux, OracleLinux, and FreeBSD • Should be capable to deploy across multiple datacenters • Should support autoscaling on the basis of CPU utilization • Platform should have capability to spin upthousands of instances in minutes • Should provide Intel, AMD based processor • Should support block storage and temporary block storage (to store Information that changesfrequently, such as buffers, caches, scratch data,and other temporary content) • Also support Block Storage Encryption			

2.	Storage	• Block Storage
		  • Block Storage must provide 99.9% SLA
		  • Block Storage should support volume snapshot
		• Object storage
		  • Object Storage must provide strong readafter write consistency
		  • Object Storage should unlimited scalestorage.
		  • Object Storage must support intelligent data tier on the basis of data use. Also havebuilt in capability to analyze storage accesspatterns to help you decide when to transition the right data to the right storage class
		  • Object Storage supports versioning andMFA for deletion.
		  • Object storage should have integration withHSM to provide inherent capability of			

		encryption			
		• File Storage • File Storage should span across multiple availability zone • Backup Storage • Archival Storage • Retrieval of Archival Storage • All the storage supports Data Encryption			
3.	Network	• Isolated Network defined at regional level mustbe able to span to multiple availability zones • Private network connectivity between VPCs, services, and on-premises applications • Securely deliver data, videos, applications, and APIs to customers globally with low latency, and high transfer speeds • Should have capability to communicate withobject storage using private network • Also supports private link between on promise tocloud infrastructure • Should provide Native Firewall with Stateful and stateless rules along with IPS capability.			

4.	Security	• CSP must provide native service for security like
		• Identity & access management
		  • Manage user access and encryption keys
		  • Single Sign on Service for Cloud
		  • Centralize Governance and Compliance Management
		• Detection Control
		  • AI Powered Threat Detection Service
		  • Unified Security and Compliance Dashboard
		  • Vulnerability Assessment
		  • Record and Evaluate Configuraion
		  • Track API and User Activity
		• Infrastructure Protection
		  • Network Firewall with IPS capability
		  • Web Application Firewall
		  • DDoS protection
		  • Central Management of Firewall Rules
		• Data Protection:
		  • Sensitive Data Discovery and Protection
		  • Encryption Key storage and Key Management (FIPS compliant)
		  • FIPS Compliant Fully managed scalable Hardware Security Module
		  • Centralize Provision, manage, and deploy public and private SSL/TLS certificates
		  • Central Store to Encrypt, Rotate, manageand retrieve secrets
		• HSM
		  • Should support FIPS 140-2 Level 3 for the storage of encryption keys ssl certificates etc. as managed service
		  • Should provide managed backup service for HSM Cluster to provide ability of restoration of keys in case of any failure ofHSM device
		• Incidence response
		  • Potential Security Threat Investigating Control
		  • Fast and Automated Control for DisasterRecovery and Ransomware Recovery			

5.	Management andGovernance	• Automate, configure and update your resources • Must have capability to enforce organizationlevel security compliance and governance • Should have capability to ensure continuouscompliance • Should trigger events and alerts on non-conformance on defined organization level governance and should have capability preventthe configuration changes.			
6.	Monitoring and Alert Management	• Should provide detail monitoring of resources and services • Should have capability to define custom alertsand matrices for resources • Ability to store log and analyse logs using SQL query statement. • Must have capability to trigger events, alerts andalarm • Must provide capability to automate			
7.	Migration	• Database Migration Service should supporthomogeneous and heterogeneous database replication • Storage Transfer Service should provide capability to extend on premise application tocloud storage, also provide capability for petabyte scale data transfer			

Advance Services:

S. No.	Service Category	Minimum Requirement	Compliance Yes/ No	Service Names and Description of the services URL	CSP Website Pricing URL of the Service
1.	Containers	• Share and deploy container software, publicly or privately • Manage containers withKubernetes • Should provide private or public dedicated container registry to store , deploy and share the containers • Should also provide platform to run container without managingservers • Should also help to containerize and migrate existing application • Cloud service should support deployment of Docker containerwith orchestration (Kubernetes/any native orchestration System)			

2.	Serverless	• Should be managed Platform • Should provide capability to scale zero to peak demands • Must have built in fault toleranceand support event driven architecture • Must have set of native servicesavailable to enable communication between decoupled components within			
		microservices, distributedsystems, and serverless applications • Must have serverless backend (compute, integration, and data stores) to run serverless workload			

3.	Managed Database Services	• It should be cloud managed platform for following database
		  • RDBMS (MS SQL server, MySQL, Postgresql, Maria DB)
		  • Graph Database
		  • Blockchain Database
		  • NoSQL Database
		  • In Memory Database
		  • MongoDB Compatible Database
		• All the database platform supports high availability and fault tolerance
		• All these database platformsshould be scalable
		• Must provide auto scalable serverless platform for MySQL and PostgreSQL
		• All these databases must supportencryption for data at rest and data in transit.
		• Database platform must supportmulti-region, multi-master replication
		• Database platform must providefull oversight of your data with multiple levels of security, including network isolation, andend-to-end encryption			

4.	DevOps	• Automatically build, test, distribute, deploy and monitoriOS, Android, Windows and macOS apps— all in one place • Developers can regularly merge their code changes into a central repository, after which automatedbuilds and tests are run. • Must provide fully managed service to implement end to endCICD pipeline • Should securely store and versionapplication's source code and automatically build, test, and deploy the application			

5.	Analytics & Visualisation Services	• Should provide managed andnative service platform for
		  • Interactive Analytics
		  • Big Data Processing
		  • Real time analytics
		  • Operational Analytics
		  • Data Visualization & Visual Data Preparation
		  • Real Time Data Movement
		  • Predictive analytics and Machine Learning			

		• Analytics service should be serverless - No need to provisionor maintain any servers. There isno software or runtime to install,maintain, or administer. • Should have built-in availability and fault tolerance. • Ingest, buffer, and process streaming data in real-time toderive insights in seconds or minutes • Handle any amount of streaming data and process data from hundreds of thousands of sourceswith very low latencies • Securely stream video from connected devices for analytics,machine learning and other processing • A built-in suggestion engine thatprovides users with recommended visualizations based on the properties of the underlying datasets. • Share business insights by packaging them up as interactivestories that users can share with others.			

6.	AI and machine learning	• Cloud service should support provisioning . Managed Service/Notebook for writing/training and support various python/R based ML library like Tensorflow, SCi-Kit, Pytorch, XGBoost • Cloud service should support Services for deploy Trained ML algorithm for inferencing • Cloud service should supportmanaged ML API for Translation, Speech, Image/Video Analysis • Must have ready-made AI capability which can be easily integrated with available appsand workflow for enhance business out come • Must provide capability to build, train, and deploy ML models • Should provide platform like TensorFlow, PyTorch, Apache MXNet, and other popular frameworks to experiment with and customize machine learningalgorithms			
7.	Internet of Things	• Should be fully managed nativeservices • Support billions of devices and trillions of messages, and can process and route those messagesto other devices reliably and securely • Connected devices can trigger events, execute predictions based			
		on machine learning models, keep device data in sync, and communicate with other devicessecurely even when not connected to the Internet • Also have capability to run and operationalize sophisticated analytics on massive volumes of IoT data • Should provide facility to secure the IoT devices • Should Provide facility to easy to collect, store, organize and monitor data from equipment's tohelp in data-driven decisions. • Should provide capability to easy to visually connect different devices and web services to buildIoT applications			

8.	Application integration tools	• Must provide native control and capabilities to
		  • Create, publish, maintain, monitor, and secure APIs atany scale for serverless workloads and web applications
		  • Create a flexible API to securely access, manipulate, and combine data from one or more datasources
		  • event-driven architecture
		  • Reliable high throughputpub/sub
		  • Should support No Code API Integration
		• Should provide managed workflow platform like Apache Workflow			

9.	Hybrid cloud	• Should help to run and manage applications wherever they mayneed to reside • It must provide infrastructure, APIs, services, and tools wherever applications may needto reside to meet low latency, local data processing, or data residency requirements. • Should have native service available to build secure andcompliant hybrid cloud architectures • Should also support cloud nativeInfrastructure services, API and tools to work seamlessly on- premise and cloud.			
10.	Media	• Fully Managed service which supports transport, prepare, process, and deliver live and on-demand content • This CSP should have services that allows the customers to buildintelligent video analytics			
		solutions that can be deployed oncloud. • Should provide capability to integrate with 3rd Party Platformfor media storage, machine learning, content protection, monetization campaigns etc.			

11.	Mobile/Mobile Application Development Requirement	• It should be fully Managed Services to create, configure, andimplement scalable mobile applications • Should supports user sign-up, sign-in, and access control to your web and mobile apps. • Must support social identity provider and custom identityprovider • Cloud service should support provisioning of Backend no SQL database for mobile application • Cloud service should support provisioning of Object Store to support uploading of binary files • Cloud service should support feature of Static Web Content hosting			
12.	Big Data	• Should provide managed platform for processing vast amounts of data using open source tools such as Apache Spark, Hivc, HBase, Flink, Hudi and Presto • Should have capability to run petabyte-scale analysis • Should also provide Platform for Data Visualization & Visual Data Preparation , Real Time Data Movement and Machine Learning			

Signature of the CSP (in case bidder is authorized partner of CSP or the bidder isCSP)

Annexure M – Technical Compliance for other Cloud related services

To
Chairman
NETF, New Delhi-110070

Subject: Submission of the Technical Compliance of other cloud related services

Dated:____/___/2023

Dear Sir,

I/We am/are the Cloud Service Provider or Authorized partner of CSP and all of our offeredother Cloud Related Service Offerings are as below:

S. No.	Service Category	Minimum Requirement	Compliance Yes/ No	Description of the services
1.	Disaster Recovery Services	As per relevant Clause (s)		
2.	Migration Services	As per relevant Clause (s)		
3.	Cloud Manage Services	As per relevant Clause (s)		
4.	Advisory Services	As per relevant Clause (s)		
5.	Capacity Building Services	As per relevant Clause (s)		

Signature with Seal of the Bidder

41. Financial Bid <u>(To be submitted in BOQ)</u>

Instructions to Bidders

1. Financial Bid shall be submitted with full price details. Financial Bid shall contain only the discount percentage and prices duly filled in as per the format given in Schedule of Rates provided in the tender document.
2. The discount percentage and prices must be quoted, failing which the Bid would be treated as unresponsive. Any discountor any other offers affecting the package price must be mentioned in Financial Bid only.
3. Price quoted by the bidder is including all transportation and installation etc. cost (if any)

Part A: CSP Services

	Percentage
Discount Percentage on List Prices (Excluding GST) of CSP as per the basic and advance cloud services in relevant clauses above Note: 1. The discount price should be eligible for all the resources and services i.e. on-demand (i.e. pay-per-hour) and long term committed resources and services. 2. Discount quoted beyond 2 decimal places is ignored	

Part B: Other Services

1. Disaster Recovery Services

Services	Unit	Unit Price (In INR)	GST Percentage	GST Amount	Total price
DR as a service to meet RTO and RPO (includes cost of VM, storage, replication, connectivity between DC & DR and any other requirement to get functional DR) Applicable when the Client is taking both DC and DR from the Cloud Service Provider. The pricing below is for the DR environment in cloud while the primary environment is functional. In case a DR is declared and the DR is scaled-up to become the new functional environment within the RPO/RTO, the Supplier will be paid for the resources provisioned as per the unit pricing of VMs for that duration.					
The cost for replication tool (including running tool, VMs required to run tool, any connectivity/storage charges)	Fixed cost Per Month				
Agent cost for replication tool	Fixed charges per VM per month				

2. Migration Services

	Unit	Unit Price (In INR)	GST Percentage	GST Amount	Total Price (In INR)
For non-database (e.g., web, application) servers	Fixed Charge Per Virtual Machine				

For database servers	Fixed Charge Per Virtual Machine				
For Database Storage	Fixed Charge Per GB				
For File Storage	Fixed Charge Per GB				

3. Cloud Managed Services

	Unit Price (In INR)	GST Percentage	GST Amount	Total Price(In INR)
% Of Monthly Bill of Cloud Services (Post Discount quoted by bidder on the CSP pricing)				

4. Cloud Advisory Service

	Unit Price (In INR)	GST Percentage	GST Amount	Total Price(In INR)
Per Person-day (Weighted average of different level of consultant deployed for the project)				

5. Cloud Capacity Building Services

	Unit Price (In INR)	GST Percentage	GST Amount	Total Price(In INR)
Online Training (Batch Size of 10 persons for oneday i.e., 6 hour)				
Offline Training (Batch Size of 10 persons for one day i.e., 6 hour) (Accommodation & Travel cost should be considered by the bidder for considering Pan India clients)				

NOTE:

- The bidder shall quote the price including all duties as applicable except GST. GST shall be paidextra as per applicable rates. NETF shall only make payment towards the GST charged in the invoice other than no other taxes/duties/charges will be paid.
- The costs quoted above shall be inclusive of costs pertaining to travel/stay and any other allowance/incidentals payable to the staff deployed by the bidder for the assignment.
- If there is any discrepancy in price quoted in figures and words, the price quoted in words shall be considered for evaluation.