HPOIL GAS PRIVATE LIMITED

(A Joint Venture of HPCL & OIL)

TENDER FOR HIRING OF CONTRACTOR TO MANAGED CLOUD SERVICE FROM AMAZON WEB SERVICES (AWS) FOR STORAGE & WEB APPLICATION HOSTING OF HPOIL GEOGRAPHIC INFORMATION SYSTEM (GIS) FOR A PERIOD OF THREE (03) YEARS

TECHNICAL VOLUME

TENDER NO. HOGPL/2024-25/C&P/008

DATE: 14.08.2024

SCOPE OF WORK (SOW)

The purpose of this tender is to invite bids from reputed organizations for Hiring of Managed Cloud Service from Amazon Web Services (AWS) for Storage & Web Application Hosting of HPOIL Geographic Information System (GIS) for a period of Three (03) Years as per following:

A. Cloud Infrastructure services (Virtual Machine Servers)			
Sl. No.	**Service Description**	**UOM**	**Qty**
1	**1 NO ON DEMAND** EC2, 4 VCPU, 32 GB RAM, 500 SSD 750 IOPS, MICROSOFT WINDOWS SERVER 2019 STANDARD 64 BIT SERVER FOR GIS ENTERPRISE SERVER	Months	36
2	**1 NO ON DEMAND** EC2, 2 VCPU, 8 GB RAM, 250 SSD 300 IOPS, MICROSOFT WINDOWS SERVER 2019 STANDARD 64 BIT SERVER FOR WEB SERVER	Months	36
3	Weekly Backup with 15 days retention	Months	36
4	Provisioning of S3 Object storage of 1TB	Months	36
5	Provisioning of network services (considering 300GB / month of data transfer i.e. 150GB / month of upload and 150GB / month of download) Billing will be done on actual data uploaded/downloaded) along with 1 No. Static IP	Months	36
6	Application Load Balancer 1(No)	Months	36
7	Domain name preferably .COM, .IN,. CO.IN, .NET, .ORG 1(No)	Months	36
8	Route 53 DNS 1(No)	Months	36
9	Provisioning of Cloud security with Antivirus (2 Nos.)	Months	36
10	1(No). Cloud watch	Months	36
11	1(No). SSL	Months	36
12	Shared Web application firewall 1(No)	Months	36
13	VPN Gateways (1Nos.)	Months	36
14	24x7 Cloud management, monitoring and support services.	Months	36
B. One-time Charges for Installation, migration, commissioning & training			
Sl. No.	Service Description	UOM	Qty
15	Installation, migration, integration, configuration, testing, commissioning, training of cloud infrastructure (One time charge)	LS	1
C. Upgradation Cost for S3 Storage			
16	S3 Storage upgrade per 10 GB per month	Nos.	720

1. MSP shall be providing various services like managed hosting (VM instances, storage, security), auto scaling, shared firewall, patch management, server administration, database administration, back-up, restore services and migration of application along with data from existing server in AWS.

2. Data/Application Migration

Currently HOGPL has its own **AWS** account and the Virtual Machines/Servers have been hosted in that account. Applications and related data are hosted in those servers. The existing AWS account is in the name of HPOIL Gas Private Limited (HOGPL). If scaling up/down of server's specification as per HOGPL current requirement in the existing account is possible, then continuation of existing account is most preferable. However, if due to any technical reason, extension of same account is not possible, then creation of new account in name of HPOIL Gas Private Limited along with the application & data migration to the new account from old account is in the scope of the Party.

The existing software's and existing status of the server is as below: -

Sl. No.	Application / Database Name	Server	Existing Server Specifications
01		Jump Server	EC2, 2 VCPU, 1 GB RAM, 30 SSD 100 IOPS , MICROSOFT WINDOWS SERVER 2019 STANDARD 64 BIT SERVER FOR WEB SERVER
02	**GIS/LIS HEXAGON SOFTWER** • Microsoft SQL-server-2019 enterprise • Project Professional 2019 • Geo Media Professional -CC • Geo Media Professional Maintenance -CC • Geo Media Web Map Professional • Geo Media Web Map Professional Maintenance • Intergraph Networks professions NL ESC • Intergraph Networks professions NL ESC Backup • Intergraph Networks professions NL ESC test • Intergraph Networks portal NL ESC • Intergraph Networks portal NL ESC Backup • Intergraph Networks portal NL test • Intergraph Networks Map Booster CC ESC-Not sold alone	GIS ENTERPRISE SERVER AND DBMS	EC2, 2 VCPU, 16 GB RAM, 140 SSD 460 IOPS, MICROSOFT WINDOWS SERVER 2019 STANDARD 64 BIT SERVER FOR GIS ENTERPRISE SERVER

	• G/Tech administrator CC ESC • G/Tech administrator CC ESC-backup • G/Tech administrator CC ESC-test		

3. Server and OS Management

- Server Remote Reboot
- OS Re-Installation/OS installation server
- OS Hardening
- OS Firewall Configuration
- On demand Server Security health check & assessment
- OS patch Management
- System log analysis
- Desiccated Technical Account Manager
- Hardware and software management

4. Application Management

- OS Firewall Management
- Anti-Virus & anti malware Protection
- MS SQL server installation
- Any software requirements for Installation

5. Monitoring and Support

- Server Ports monitoring
- 24/7/365 days Support
- Server Resource Monitoring (CPU, RAM, DISK, etc.)
- Internet Bandwidth Report and Monitoring
- Cloud watch and Monitoring service
- Load Balancers monitoring
- Web Application Firewall monitoring

6. Backup Management

- Backup agent Installation and Configuration
- Basic Support
- Basic Monitoring
- Backup health check
- On Demand Restoration of backup on same source machine
- Advance Backup protection service
- Entire VM data backup must be available.
- Weekly Backup with 15 days retention.

- 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.
- Data backup VMs, Microsoft SQL, Application, All Data backup
- Disaster Recovery

7. Replication Management

- Replication Configuration
- Replication monitoring
- Troubleshooting replication issue
- Failover/Failback
- Data recovery availability for CSP.

8. Database Management

- Proactive monitoring
- Configuring Database Backup and Recovery
- Database maintenance
- Database Incident and problem Management
- Configuration and Deployment of Report servers.
- Data base setup and management Microsoft SQL
- Configuration database mirroring
- Storage Management

9. SECURITY – SHARED RESPONSIBILITY

- One number Domain Name Registration Service One
- One number Domain Wildcard SSL certificate
- Antivirus 2
- System log should be available.
- Cloud watch
- Web Application Firewall
- Monthly Report Summited.

10. Network & Connectivity Services.

- Static Public IP (1Nos.)
- Minimum 20 Mbps Internet bandwidth on cloud with DDOS protection
- Layer 7 Load Balancers
- VPN Gateway
- Route 53(DNS)

11. CSP Provided Cloud Infrastructure Implementation.

- The bidder must provide the GIS architectural structure of the system to the buyer and the same must be approved by the EIC before installation of the system.

12. Evaluation of existing infrastructure and migration into Cloud, necessary support backup database shall be provided by bidder.

13. SPECIFICATIONS FOR REQUIRED CLOUD BASED SERVICES

A) Enterprise GIS Server and DBMS (Qty: 1 no)

Sl. No.	Parameters	Description
1	**Operating System**	Microsoft Windows Server (2019 Standard 64 Bit Edition)
2	**Storage in GB**	500 SSD
3	**RAM in GB**	32
4	**VCPU**	4
5	**IOPS**	750
6	**Data Backup Storage**	**1 TB SSD**

B) Web Server (Qty: 1 no)

Sl. No.	Parameters	Description
1	**Operating System**	Microsoft Windows Server (2019 Standard 64 Bit Edition)
2	**Storage in GB**	200 SSD
3	**RAM in GB**	8
4	**VCPU**	2
5	**IOPS**	300

C) Provisioning:

Sr No	Description of Service
1	Static Public IP (1 Nos.)
2	Application Load Balancer
3	Web Application Firewall Configuration
4	One number Domain Name Registration Service
5	Domain Wildcard SSL certificate 1
6	20 Mbps Internet bandwidth on cloud with DDOS protection
7	Antivirus 2

8	Weekly Backup 15 Days retention
9	Route 53 DNS
10	Cloud Watch
11	VPN Gateway (1)

14. Upload/Download Requirements:

- Clarity on Upload / Download charges if any is required, per GB price to be indicated. Bidder has to quote for 300 GB / month of data transfer i.e. 150GB / month of upload and 150GB / month of download.
- Bulk data transfer during initial project migration and during exit management should be carried out using secure practices where the data is encrypted. Price for bulk data transfer should be indicated.

15. Compliance:

Sr No	**Cloud Scope**	**YES/NO**
1	MSP Will be Responsible for procuring and maintaining the cloud services including migrating to cloud and managing cloud service.	
2	It is the responsibility of the MSP to monitor the cloud services (Resource management user administrator performance service levels etc.	
3	Establishing connectivity between user Department premise to cloud DC and DR site. Data recovery strategies shall include appropriate redundancies including off-line data backup weekly	
4	Deploying new supplication on cloud user administrator, security administrator planning and implementation of cloud management and monitoring portal for complete infrastructure and service procure	
5	Monitoring Reporting Service	
6	Exit management and billing management will be done by MSP	
7	Computer services and provisioning, installation, configuration, communication, de-communication and management the virtual machine and provide user department the access to the same via secured web browser.	
8	Storage service provisioning of scalable storage capability as per requirement of the client and the availability for service	
9	Managed data base service setting up, installation, configuration, management upgradation and migration of database service	
10	Network Service: Maintain and manage the required network components for the cloud service procured by the client.	

11	Security service provisioning, installation, configuration, management, monitoring of security service asked for the requirement of user department.	
12	Disaster recovery plan and implication, setup and configuration of virtual VMS, storage, network, database, etc. etc. DR site meeting PRO and RTO requirements of the user department	
13	Monitoring and reporting service: Deploy against basic monitoring and tracking system user and user report.	
14	The underlying project infrastructure, any additional hardware and software require for cloud operations shall be provided by MSP for cloud service along with management of application suite.	
15	MSP and CSP will be responsible for the cloud service.	
16	MSP shall host application on Cloud.	
17	Consult with user department to understand business requirement.	
18	Conduct functionality teat	
19	The CSP should be MEITY empanelment who are audit complaint.	
20	MSP should submit the MAF which must be valid for the entire contract period. If the MAF with AWS is not valid for the full contract period, then the MSP should give a self- declaration that he will extend the validity of MAF with AWS for the entire contract period.	

16. Security Features:

During the contract period, the following conditions should strictly be met. Any change/ variation in these conditions should be notified to HOGPL immediately. Reports of periodic audits and certifications should be made available online or shared on demand for scrutiny.

- CSP/MSP should provision proposed resources strictly from India Regions
- CSP should maintain accreditation by MeitY
- CSP should maintain below security compliance certification.
  - ✓ ISO/IEC 27001 (Information Security Management)
  - ✓ ISO/IEC 27017(Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology)
  - ✓ ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds.)
  - ✓ PCI DSS - Compliant technology infrastructure for storing, processing and transmitting credit card information in the cloud
  - ✓ SOC 1, 2 & 3 (Service Organization Controls Standards for Operational Security)
  - ✓ MeitY Certification
  - ✓ Compliance with the IT Act 2000
  - ✓ Data Residency in India
  - ✓ Data Security Compliance
  - ✓ Tier – III Compliance

- ✓ ISO 20000_1
- ✓ ISO 20000_9

- The CSP/MSP shall meet all the security requirements, as applicable to HOGPL, indicated in the IT Act 2000 and its subsequent amendments, the terms and conditions of the Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC.
- The CSP/MSP should be capable of encryption of the data at rest and in transit and follow security guidelines as directed by HOGPL.
- At the end of the agreement, the CSP/Service Provider shall ensure that all the storage blocks or multiple copies or any back up (online/offline) of data, if any, are unallocated or zeroed out, so that data cannot be recovered.
- The CSP/MSP undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated/ published/advertised by the CSP/MSP to any person/organization without the express permission of HOGPL.
- The Indian Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency after informing HOGPL.
- The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC/MeitY guidelines as and when published). If the services are not meeting the STQC/MeitY guidelines, HOGPL shall have the option to discontinue the service and/or entire contract.
- The Audit, Access and Reporting Requirements should be as per the terms and conditions of the MeitY Empanelment of the Cloud Service Provider.
- CSP to provide us the Read-Only-Access for Audit purposes.

MSP: PROJECT IMPLEMENTATION

a. Requirement Gathering and Finalization: MSP will undertake Discussions with Department to understand the project requirements.
b. Note: This is a continuous and on-going activity and based on the requirements of HOGPL, MSP needs to provide the VPC cloud services.
c. MSP to understand from HOGPL IT team the existing workloads and existing applications running in existing AWS cloud which are to be migrated etc.
d. Discussion with the department for finalization of requirement: Post discussion and consultation between Department, MSP to finalize the To-Be state along with Migration plan and requirements and provide recommendations, if any.
e. Prepare a Project Roadmap along with timelines and deliverables.
f. Design, configuration, installation, application profiling and mapping, identifying the service module (IaaS, PaaS, SaaS), setting up of Cloud site.
g. Domain Web hosting and integration with Cloud service.
h. Managed Cloud Services including infrastructure deployment, set-up, migration etc.:
i. ✓ Implement the services (as defined in the Scope of Work in this proposal), GIS/LIS, Deploy services on cloud, Support etc.
j. ✓ Migration of real time and archival data from on-prem / existing data center/existing CSP will be the responsibility of MSP.
k. h. Management Support: Platform Monitoring, Performance tuning, Cost optimization, Update/upgrade management, Break fix management, Change management, Incident management, SOC management, Threshold based alert, Access management, Patch management (for managed services), Backup management, Monthly reports.
l. HOGPL and Support: Regular Reporting and Periodic Meeting Maintenance & support of implemented Cloud Sites as per the defined SLAs.

TRAINING

i. The successful bidder shall make arrangement for training of on system administration at purchaser's premises as per mutually agreed training plan under the scope of work as below:
ii. On-site / Virtual for 2 days, as per mutually agreed terms and conditions as described below:
iii. Training on operations, maintenance, support & administration for software /hardware / Database / OS / Middleware, application architecture and all other related components.
iv. Configuration and functionalities required for implementation of various utilities and features and deployment of new and existing applications.
v. Performance tuning of application / database / middleware etc.
vi. Training manuals for hands-on training shall be prepared and handed over to the purchaser before the start of the training.
vii. Training shall be provided by OEM / CSP/MSP certified trainers.

INSTALLATION

a) The Bidder shall configure the solution as per the detailed scope mentioned in this document and further can be improved based on the discussions held at SITE with HOGPL Team.
b) The successful bidder shall be responsible for execution of the jobs envisaged for "Implementation of

c) Cloud Based Infrastructure for IT applications at HOGPL.
d) The scope of work shall cover creating compute, network, and storage resources, installation,

integration, configuration, testing, commissioning of the applications and data infrastructure, documentation, stabilization, demonstration of performance guarantee and putting into satisfactory operation with defined uptime and quality of services of cloud on "Infrastructure as a Service".

e) The configurations shall be done by the bidder with the help of expert engineers. The bidder needs to submit the certificate stating that best practices have been followed in installation and configurations.
f) The Bidder will support in the implementation, management and monitoring of VPC infrastructure which is to be configured for the application and ensure 99.5 % uptime of services as per agreement.
g) The Bidder will be responsible for migrating to cloud in co-ordination with the HOGPL IT team and should ensure to meet all standard data formats for data transfer.
h) The bidder shall be responsible for monitoring the cloud services.
i) Bidder shall provide cloud engineer / cloud professionals throughout the contract period to support HOGPL as and when required. The Cloud engineer should be available for physical meetings, requirement gathering, project discussions as well as during migration process with HOGPL team as and when required and communicated by HOGPL.
j) Service provider shall be responsible for security of resources, Network infrastructure along with implementation security compliances.
k) Service provider shall be responsible for any Risk Management and planning, or issues related to migration of data from DC to DR as per the requirements.
l) Service provider shall provide necessary technical documentation, design documentation, standard Operating Procedures (SOPs) required for operations and management of services.
m) The bidder shall provide the relevant reports, including real time as well as past data / reports on dashboard.
n) Provide report on utilization and optimization of the resource.
o) Provide portal logins for billing, provisioning, usage etc. as per the requirement of the projects also the bidder will provide the access of root account of proposed CSP to HOGPL.
p) The bidder will provide the dashboard for monitoring and financial aspects asper the bid document requirement.

ACCEPTANCE TESTS (AT)

A. Checking of the Configuration as per the technical specifications.
B. Running & Server the diagnostic tests for systems to check for the specifications.
C. The complete functionality of the system shall be tested as per Scope of Work & Technical Specifications.
D. Checking for successful running of migrated existing applications (HEXAGON)
E. along with data in the new VMs.

SUPPORT AND MAINTENANCE SERVICES

a. The Vendor shall be responsible for the entire solution for trouble free operation during the support & maintenance services period of 03 years. Zero date for support & maintenance services will start only after signing of Acceptance Protocol by bidder's representative and EIC.
b. The successful bidder has to manage and maintain the VMs including underlying hardware, operating systems, security etc. for the contract period. The successful bidder shall be required to provide all technical support during the contract period for maintenance of cloud infrastructure service.
c. During migration and support period, new/latest patches update to be made available with no additional costs.
d. The successful bidder shall submit technical documentation of cloud infrastructure set up that includes information and details about the components and configuration settings.

e. MSP Support services is defined as Support services from the Managed Services from the partner.
f. MSP Support services for Cloud Support includes (indicative list), Platform Monitoring, Performance tuning, Cost optimization, Update/upgrade management, change management, Incident management, SOC management, Threshold based alert, Access management, Patch management (for managed services), Backup management, Monthly reports.
g. The system shall be designed to be scalable to accommodate the additional requirements of hardware and software resources for future requirement.
h. There shall be one mobile number, online web portal and e-mail ID wherein call can be booked 24 x 7. The Non-performance Deductions shall be calculated from the call booked time to the call resolved time and cumulatively all the down times shall be added, and the Non- performance Deductions shall be quarterly calculated accordingly.
i. Provide support at any time (24 hours a day, 7 days a week) via all possible modes including phone, chat, and email support to TIA for provisioning and configuring cloud resources.
j. All necessary tools, tackles and accessories required to complete the scope of work as per tender document is in the scope of the bidder, at no extra cost to HOGPL.
k. The bidder should have the necessary self-service portal & various process automation tools for monitoring, administration (Start/ Stop) etc. of AWS resources.

NON-PERFORMANCE DEDUCTIONS

The bidder is required to adhere to the Service Level Agreements as mentioned below:

Sr. No.	Service Level Objective	Definition	Target	Penalties
1.	Availability of each cloud service (Applicable for all Cloud Service as defined in Cloud Services Bouquet)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month: (Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the cloud service>=99 .5%	Penalty as indicated below (per occurrence): a) = 99.00% - 10% of Quarterly Payment of the Project b) = 98.50% - 15% of Quarterly Payment of the Project c) = 98.00% - 20% of Quarterly Payment of the Project d)
2	Availability of Critical Services(As defined in Annexure B) *This SLA shall not be applicable when the associated cloud service as mentioned in SLA#1 above is not available /up.	Availability means, the aggregate number of hours in any specified time period during which the critical service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime	Availability for each of the critical service>=99 .5%	Penalty as indicated below (per occurrence): a) = 99.00% - 5% of Quarterly Payment of the Project b) = 98.50% - 10% of Quarterly

		Calculation for the calendar month:{[(Uptime Hours in		Payment of the Project c) =

		the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}		98.00% - 15% of Quarterly Payment of the Project d)
3	Availability of regular reports (SLA , Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Penalty as indicated below (per occurrence): a) <11 working days to >= 6 working days - 2% of Quarterly Payment for the Project b) <16 working days to >= 11 working days - 4% of Quarterly Payment for the Project c) For the delay beyond 15 days , penalty of 5% of the Quarterly Payment for the Project
4	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use Uptime Calculation for the calendar month:{[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in	Availability of the Cloud Management Portal of CSP >=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of

		the calendar month] x 100}		Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the Quarterly Payment of the Project.
5	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core) Measurement shall be done by analyzing the log files	95% within 5 minutes	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Service b) <90% to >= 85.0% - 10% of Quarterly Payment of the Service c) <85% to >= 80.0% - 15% of Quarterly Payment of the Service d) <80% - 20% of the Quarterly Payment of that Service

6	Spinning up the Object Storage	Time to spin up Object Storage Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service
7	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service

8	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports.	No more than 15 minutes lag between usage and Cloud Service (API) reporting, for 99% of Cloud Services consumed by the Government Dept	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project
9	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports and Invoices	No more than 24 Hrs. of lag between availability of cost details and actual usage, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project

10	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with Government Dept. within 5 working days of vulnerability identification. Measurement period is calendar month	Percentage of timely vulnerability reports shared with Government Dept. within 5 working days of vulnerability identification>= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project
11	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. a) High Severity - Perform vulnerability correction within 30 days of vulnerability identification. b) Medium Severity - Perform vulnerability correction within 60 days of vulnerability identification. c) Low Severity - Perform vulnerability correction within 90 days of vulnerability identification. Measurement period is calendar month.	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project
12	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud based services and components are compromised or any case wherein data theft occurs (includes	No breach	For each breach/data theft, penalty will be levied as per following criteria.

		incidents pertaining to CSPs only)		1. Severity 1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity 2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity 3 (as define in Annexure A) - Penalty of Rs 5 Lakh per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << Government Department / Agency>> reserves the right to terminate the contract
13	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual		

		infrastructure and applications. Denial of Service Attack: This shall include non-availability of any of the Cloud Service due to attacks that consume related resources. The Service Provider shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of		
14	Response Time under Basic Support (As defined under cloud service bouquet	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 60 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 2%

				of Quarterly Payment of Basic Support service
15	Percentage of timely incident report under Basic Support service(As defined under cloud service bouquet	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 1 Hr. of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Basic Support service
16	Response Time under Enterprise Support (As defined under cloud service bouquet)	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	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 9% of

				Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Enterprise Support service
17	Percentage of timely incident report under Enterprise Support service(As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 15 min of occurrence	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Enterprise Support service
18	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 95% of the incidents should be resolved within	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of

			30 minutes of problem reporting	Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
19	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	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment ofthe Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
20	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa	RTO <= 4 hours Government Department may specify more	10% of Quarterly Payment of the Project per every additional 2 (two) hours of downtime

			stringent RTO based on its application requirement	
21	RPO (Applicable when taking Disaster Recovery as a Service from the Service Provider	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours Government Department may specify more stringent RPO based on its application requirement	10% of Quarterly Payment of the Project per every additional 2 (two) hours of data loss
22	DR Drills	At least two DR drills in a year (once every six months) or as per the agreement	At least two DR drills in a year (once every six months) or as per the agreement	a) No of DR Drills =1 - 1% of the Yearly Payment of the Project b) No of DR Drills = 0 - 2% of the Yearly Payment of the Project These will be measured every six months and the liquidated damage will be levied at the end of year
23	Data Migration	Migration of data from the source to destination system	Error rate < .25%	a) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the Project b) Error Rate > 0.30% & <=0.35% - 2% of the

				Quarterly Payment of the Project c) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the Project For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the Project will be levied as additional liquidity damage
24	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.0% - 10% of Quarterly Payment of the Project c) <85% to >= 80.0% - 15% of Quarterly Payment of the Project d) <80% - 20% of the Quarterly Payment of that Project

25	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage based threshold Measurement shall be done by analyzing the log files	99% within 10 mins of crossing the Threshold	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 0.25% of Quarterly Payment of the Project b) <95% to >= 90.0% - 0.5% of Quarterly Payment of the Project c) <90% to >= 85.0% - 0.75% of Quarterly Payment of d) <85% - 1% of the Quarterly Payment of that Project
26	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project duration. Service Provider should ensure the sustenance / renewal of the certificates	All certificates should be valid during the Project duration	Delay in sustenance of certifications a) > 1 day & <= 5 days - 1% of the Quarterly Payment of the Project b) > 5 day & <= 15 days - 2% of the Quarterly Payment of the Project c) > 15 day & <= 30 days - 5% of the Quarterly Payment of the Project d) > 30 days, 10% of the Quarterly Payment of the Project

27	Non-closure of audit observations	No observation to be repeated in the next audit	All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 5% of the Quarterly Payment of the Project b) > 10 % & <= 20% - 10% of the Quarterly Payment of the Project c) > 20 % & <= 30% - 20% of the Quarterly Payment of the Project d) >30% - 30% of the Quarterly Payment of the Project

OTHER TERMS & CONDITIONS

- After placing the FOA, the vendor shall submit the detailed Project Schedule to the Engineer-In-Charge stating the dates and activities planned including the details of the engineers that will be deployed for the installation and configuration of the solution. The schedule shall be having the clear details of the dates and the engineers visiting the site
- All necessary tools and accessories required to complete the scope of work as per tender document is in the scope of the Contractor.
- In order to establish the claims made by the bidder, they are required to submit documentary evidence / references which are must for evaluation of bid in a transparent manner. Bidder should necessarily provide the documentary evidence supporting the technical specifications of the offered solution, as asked in various places in this document. Failing to submit the requisite documents may lead to summarily reject the bid and HOGPL do not intend to provide any second chance.

9. EXIT CLAUSE

Exit Management and Transition Requirements Listed below are mandatory.

a) If the services given by the successful bidder during the contract period are not found satisfactory, then HOGPL reserves the right to terminate the contract.
b) In case the work is kept suspended without any valid reason, HOGPL shall be free to get the remaining work executed through any other agency.
c) Continuity and performance of the services at all times including the duration of the agreement and post expiry of the agreement is a critical requirement of the HOGPL. It is the prime responsibility of the successful bidder to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility /service shall be affected / degraded. Further, the successful bidder is also responsible for all activities required to train and transfer the knowledge to the HOGPL to ensure similar continuity and performance of the services post expiry of the agreement.
d) At the end of the contract period or upon termination of contract, the successful bidder is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of HOGPL without any extra cost.
e) The successful bidder shall support HOGPL in migration of the VMs, data, content and any other assets to the new environment created by HOGPL or any agency (on behalf of the HOGPL) on alternate cloud service provider's offerings to enable successful deployment and running of applications of HOGPL on the new infrastructure. The service provider shall have the responsibility to support and assist HOGPL till it is able to successfully deploy and access the services from the new environment.
f) The successful bidder shall not delete any data at the end of the agreement (for a maximum of 60 days beyond the expiry of the agreement) without the approal of the HOGPL. Further the bidder shall facilitate the DBMS from exiting to new server at the end of the contractual period. The successful bidder has to ensure that data is not compromised during the exit process. Also, the successful bidder has to provide data in a reasonable format that is capable of being utilized by any new service provider.
g) During the exit/transition management process, it is the responsibility of the successful bidder to address and rectify the problems with respect to migration of the applications and related IT infrastructure including installation / reinstallation of the system software etc.
h) The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with HOGPL.
i) During the contract period, the successful bidder shall ensure that all the documentation required by HOGPL for smooth transition including configuration documents are kept up to date and all such documentation is handed over to the purchaser during the exit management process