GIPL is a leading Total Solution Provider of IT/ITeS services to Government of Gujarat and its Corporations/ Boards. We are ISO 9001:2015 certified origination and a subsidiary of Gujarat State Petroleum Corporation Ltd (A Govt. of Gujarat Undertaking).Guj Info Petro Limited(GIPL) has been providing various IT related Services, IT Project Consultancy as a Total Solutions Provider / Nodal Agency to Government of Gujarat and its Corporation / Boards, Educational Institutions etc. since more than 15 years.

GIPL is looking forward to select Service provider for "Web based software application for Gas consumption data sharing and Server**" as per Scope of work and Technical Specification mentioned in Annexure - B.**

In this regards, we request you to provide quotation for said services in the following format for "Web based software application for Gas consumption data sharing and server" **on or before - 05/10/2019, 3.00 PM in sealed cover, with duly mentioned thereon** "Web based software application for Gas consumption data sharing and Server for GIPL's Client**" at the below address.**

Address:
Guj Info Petro Limited
Block 15, 2nd Floor, UdhyogBhavan,
Sector 11, Gandhinagar
Gujarat 382011
Kind Attention: CPO

A. Commercials:

Sr. No.	Description	Amt. Without taxes	GST	Tax AMT	TOTAL Amt. With Taxes
		(A)	(B)	(C)=A x B/100	(D)=A+C
1.	**Web based Application for sharing of Gas Consumption Data to client**				
2.	Server Hardware: **Intel(R) Zeon Processor, 16 GB Ram, 256 GB SSD plus 2TB 7200 RPM SATA, Microsoft Windows Server OS and 3 years onsite warranty.**				
Total Amount (Inclusive of Taxes)					

❖ Hosting requirements
  ▪ **Hosting infrastructure as per suggestions from Vendor shall be provided by GIPL's Client for said application. The server hardware as per below mentioned specification shall be utilized for the same.**

Application Server / Database Server Requirements

Component	Recommended Specifications
Server Hardware	**Intel ® Xeon Processor, 16 GB Ram, 256 GB SSD plus 2TB 7200 RPM SATA**
Operating System	**Windows Server 2008 R2 or higher**
Database Server	**MS SQL Express**
Reports	**SQL Server Reporting Service (Latest Version)**

❖ Project Timeline

It is expected that the project will be completed in <u>1 Months approximately</u> from date of work order. However, any delay due to change / addition in requirements, delay in approval from GIPL's, Client shall have proportionate effect on projected timeline and the same shall be considered on mutual agreement.

B. Eligibility Criteria

1. **The Service provider must have valid PAN and GST registration.**

2. **The Service provider should have no record of being black-listed by any Government/ Public Sector/ Multinational/ National companies. (Self-declaration Certificate as per** Annexure-A **enclosed herewith)**

3. **Evaluation will be based on Bidder's eligibility and the most competitive and the lowest rate quoted by the participating and eligible bidders.**

4. **Any clarifications desired by any Service provider in connection with any part of this inquiry may be sought as per contact details below, however no bid will be acceptable by e-mail.**

5.

Name of Contact Person	Contact email ID
Tapansinh Mahida	**tapansinh@gipl.net**

Terms & Conditions:

A. General:

a. **Proposed rates should be exclusive of taxes. Any taxes, as may be applicable at the time of invoicing will be charged extra on above rates. Currently GST at the rate of 18% is applicable.**

b. **Above Prices include on-site implementation support also.**

c. **Hosting of said application is not in scope of this inquiry and the proposed server will be hosted at existing GIPL's Client server room.**

d. **Vendor will be responsible for any problem arising due to Wrong Inputs by users, etc.**

e. **Vendor shall not be liable for any data entry work of any records. If required the same shall be done on chargeable basis.**

f. **Vendor may propose cost based on the scope stated in the Scope of Work section. No deviation in scope of work shall be allowed.**

g. **Vendor shall ensure and maintain the schedules mentioned in this inquiry and Vendor will make all reasonable efforts to meet this objective.**

h. **Any licenses if required for the software/hardware/Operating System etc. other than specified in scope of this inquiry shall be purchased by GIPL's client separately.**

B. Delivery

- **On receipt of the firm Purchase Order, Vendor shall initiate the project within 7 days.**

C. Payment

Payment terms for Software Development:

- **30 % upon submission of SRS document**
- **30% upon installation & Commissioning**
- **40% after 3 months successful run after Go-live**

The payment shall be made within 15 days from date of receipt of Invoice as per milestones achieved.

D. Support & Annual Maintenance Contract of (AMC)

- **Vendor shall provide 1 year warranty support from the date of commissioning. The support shall include only rectification of errors or bugs encountered during usage.**
- **Any modifications/enhancements/additional features to the implemented system shall be charged extra as per mutual agreement & shall be treated as change request.**
- **After initial support period of 1 year, AMC shall be signed at the proposed rate by vendor.**

E. Validity

The prices are valid for 60 days from the date of the inquiry.

F. Training

Vendor shall provide single day user training at a single site, unless mentioned otherwise in this document. "Train the Trainer" approach shall be taken to conduct the user training.

G. IP Policy:

Source code and IP rights of the software developed shall be of GIPL. The vendor shall not use the same for any other client with or without commercial value without written permission of GIPL.

H. Confidentiality:

Any information, guidelines, relevant rules & regulations etc. provided by Client under and pursuant to this engagement shall not be disclosed or referred to publicly or to any third party by vendor except in accordance with prior written consent of Client. Client also agrees to keep confidential the proprietary and other information of vendor derived during the course of the engagement.

However, Client and vendor shall not be bound by the confidentiality obligation if information is required by any regulatory or statutory authority or a court of competent jurisdiction.

I. Governing Laws & Jurisdiction

The resulting engagement shall be made under, and shall be governed by and construed in accordance with the laws of India and will be subject to exclusive jurisdiction of courts in Gandhinagar, Gujarat, India.

J. <u>Limitation of Liability</u>

GIPL's total liability to the service provider over the period of the resulting engagement arising out of or in connection with the engagement whether such liability arises from any claim based upon contract, warranty, tort or otherwise, shall in no case exceed 100% of the actual amount to the paid by Guj Info Petro Limited to the service provider under the resulting engagement. In no event shall GIPL be liable for any incidental damages, consequential damages, special damages, indirect damages, loss of profits, loss of revenues, or loss of use, these limitations and exclusions will apply regardless of whether liability arises from breach of contract, warranty, tort (including but not limited to negligence), by operation of law, or otherwise.

K. <u>Liquidity Damage</u>

a. **If you fail to deliver and install the requisite software application and Hardware within 1 month from the issue of the purchase order, then a sum equivalent to (0.5%) of the total contract value shall be deducted from the payment for each calendar week of delay or part thereof subject to maximum 10% penalty.**

b. **Delay in excess of 1 month will be sufficient to cause for termination of the contract**.

<u>Security</u>

A secure Web application relies upon a secure infrastructure. Network consists of routers, firewalls, and switches; host consists of operating system, operating system's runtime services, runtime components, virtual machine; and application consists of web server, container, scripting engine and application binary. Securing n/w components is responsibility of infrastructure management team, securing host and web server is responsibility of web server admin and securing application is responsibility of programmer.

<u>Measures for security of web based applications</u>

Following are some of the measures recommended for the security of the web based applications:

- **Authentication: Authentication mechanism devices a process of "introducing" and validating the user to a web application and hence forms the first layer of defense for the web application. The robustness of the authentication mechanism must be ensured for building a secure web application.**
- **Authorization: If the restrictions on what authenticated users are allowed to do are not properly enforced, attackers can exploit the flaws to access other user's accounts, view sensitive files, or use unauthorized functions. Therefore, the authorization of user access must be clearly defined and built in the application.**

- **Error and Exception handling:** Error conditions that occur during normal operation should be handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, and cause security mechanisms to fail.
- **Input validations:** The information received by the web applications from the web-requests must be properly validated before being used by a web application. Attackers can tamper the request or part of the request to cause the application to misbehave. Just having very strong input validations can easily prevent many types of attacks.
- **Session Handling:** Attackers that can compromise session cookies and other session related information can defeat authentication restrictions and assume other user's identities. Therefore proper session handling mechanism should be in place.
- **Encryption and Cryptography:** Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them are difficult to design, and may result in a weak implementation.
- **Physical security:** The computer running the web server should be kept physically secured in a locked area. Any backup storage media (tapes, removable disks, etc.) should be similarly protected.

Key Components of Security

Application Security

Each application will be categorized by the following set of attributes.

- **Type of work (Application Development & Maintenance / Production support)**
- **Availability commitments; i.e. how mission-critical is this application, which in turn will drive the following.**
  - **Distribution of responsibilities between data center and implementation site teams**
  - **Dependence on communication facilities**
  - **Disaster Recovery Strategy for application data (as applicable)**

Affiliations & Standards

- **The keys to sound security are often considered to be: deployment of a sensible security risk analysis approach, compliance with a recognized standard such as ISO 9001:2008, development of comprehensive information security policies and deployment of a detailed security audit program.**

Virus Protection

- **Two tiered approach towards protection from Virus is recommended**
- **Usage of two different anti-virus products ensures that in case any virus escapes any one Antivirus, the other product will take care of that.**
- **Dedicated Infrastructure Development team managing the Anti-virus definition servers.**
- **Daily update of antivirus definitions.**
- **Desktop Antivirus clients and Server configured in classical push pull technology.**
- **Daily Scheduled Scans**
- **Patch management Process is very clearly defined and strictly followed and reviewed**
- **Use of enterprise security manager software to check policy compliance**
- **Use of patch management soft wares**
- **Separate testing environment before deploying patches**
- **Dedicated Infrastructure Team to test, Install and Review the patch management status**

Performance:

- **The performance of the web based systems is of utmost importance as the users are located at remote locations and connecting through a browser window. The speed of refreshing the data, web pages, uploads and download speed etc has been considered for better performance. A minimum performance standard has to be decided upon and further tuning of both the hardware and software has to be undertaken for better performance.**

Scalability:

- **Since the government business is very dynamic, the scalability issues have to be given due importance. The system architecture defined for SWD (3-tier architecture) helps in scaling of the system horizontally, vertically and diagonally. Horizontal scaling is characterized by rapid application development, but simplified change management. Horizontal scaling can help organizations achieve the right level of resilience. With vertical scaling, services are scaled within the system — resources such as CPUs, memory, and storage can be incrementally added to the server over time to increase scalability. Vertical scaling is characterized by slowly changing applications and is often necessary for data-intensive services such as databases, video servers, mail stores, and directories. Diagonal scaling is a combination of horizontal and vertical scaling. Each server in the group of horizontally scaled servers can be grown within the system, providing increased flexibility.**

Thank you and we look forward to receiving your quotation.

GIPL TEAM.

FORMAT FOR SELF DECLARATION – NO BLACKLISTING CERTIFICATE

No: Date: <DD/MM/YYYY>

To
Chief Executive Officer
Guj Info Petro Limited
Block No: 15, 2ⁿᵈ Floor, Udyog Bhavan,
Sector -11, Gandhinagar – 382 011, Gujarat.

Ref: "Web based software application for Gas consumption data sharing and Server for GIPL's Client"

Dear Sir,

In response to the referenced **"Web based software application for Gas consumption data sharing and Server for GIPL's Client",** as an owner/partner/director of _____ _____, of _____ _____, I/ We hereby declare that presently our company/firm _____ is having unblemished record and is not declared ineligible for corrupt and fraudulent practices either indefinitely or for a particular period of time by any State/Central Government/PSU.

We further declare that presently our company / firm _____ is not blacklisted / banned / declared ineligible / declared having dissatisfactory performance / put on holiday list / disqualified for reasons of corrupt and fraudulent practices by any State/Central Government/ PSU on the date of Bid submission.

We further declare that presently our company / firm _____ is not blacklisted by any State/Central Government/ PSU for any IT/ITeS Goods and/or Services as on the date of Bid submission.

Yours Sincerely,
Name of the Bidder:
Authorized Signatory:
Seal of the Organization:
Date:
Place:

Annexure – B: SCOPE OF WORK:

- **Development of scalable, accessible and secured web portal for sharing real time gas consumption data to Clients customers/stack holders/management.**
- **Development of scalable web portal for sharing real time as well as historical data of customers/suppliers in tabular/graphical format.**
- **Supply necessary hardware and software to host developed application.**

DEVELOPMENT MODULES:

- **Following modules are to be development as per scope defined hereunder:**

1. Admin User & Login Module:

   - **Login page for secured and user specific access.**
   - **Based on rights, there will be two type of users:**

     I. Client: **This type of user will include customer/Base/Sub Base. This type of user will have only data viewing rights.**
     II. Administrator: **This type of user will have all rights which including customer add/edit/delete, password change, user id creation.**

2. Customer/Supplier Add/Edit/Delete

   - **Only administrator will have right to access this module.**
   - **Each supplier/customer will have following basic information:**
     I. **Customer/Supplier Name**
     II. **Address**
     III. **Contact Person**
     IV. **Mobile No**
     V. **Email Id**
     VI. **User Id & Password**
     VII. **Base/Sub Base Name**
   - **Checkbox will be provided for selection of type supplier/customer.**
   - **For suppliers, user id and password will not be created but same will be available in base/sub base/administrative accounts.**
   - **Option for creation of meter.**
   - **Option for assignment of average GC values from dropdown/checkbox.**

3. Meter Add/Edit/Delete, Tag add/edit/delete:

- **Each customer/supplier will have different number of meters.**
- **While adding meter, administrator will be allowed to add following information:**
    - I. **Assignment of unique tag/key for all the parameters in the list. (List of default parameters will be preloaded.)**
    - II. **Checkbox to customize which parameter is to be provided to customer user id for viewing.**

4. GC parameters ad/edit/delete

- **Addition of GC parameters from standard list to be provided by client.**
- **Assignment of identification tag of real time as well as average parameters.**
- **Assignment of necessary Base and Sub Base.**

5. Base/Sub base Add/Edit/Delete

- **Add/Edit/Delete of Base accounts.**
- **Add/Edit/Delete of Sub Base accounts.**

6. Tabular/Graphical interface for Client's management:

- **Homepage with live ticker of large customers/suppliers.**
- **Separate page for each customer/supplier.**
- **Maximum, minimum and average data of each customer/supplier.**
- **Historical tabular/graphical data.**
- **Live graphical data.**

INFORMATION to be provided by client

- **List of parameters to be configured in meter.**
- **List of parameters to be configured in GC.**
- **List of Base/Sub base**
- **Copy of sample Database in csv/json/sql format.**

DEVELOPMENT TOOLS:

Following development tools will be utilized/used for development of required application:

- Server**: Node.js, Express**
- Database**: PostgreSQL, MongoDB**
- Front End**: React.js with Redux, CSS3**
- Login Security**: JWT (Json Web Token) authentication**

HOSTING INFRASTRUCTURE CONFIGURATION:

- Processor: **Intel XEON processor.**
- RAM: **16 GB RAM.**
- Storage: **256 GB SSD, 2 TB HDD**
- Operating System: **Microsoft Windows Server OS.**

Security

A secure Web application relies upon a secure infrastructure. Network consists of routers, firewalls, and switches; host consists of operating system, operating system's runtime services, runtime components, virtual machine; and application consists of web server, container, scripting engine and application binary. Securing n/w components is responsibility of infrastructure management team, securing host and web server is responsibility of web server admin and securing application is responsibility of programmer.

Measures for security of web based applications

Following are some of the measures recommended for the security of the web based applications:

- **Authentication: Authentication mechanism devices a process of "introducing" and validating the user to a web application and hence forms the first layer of defense for the web application. The robustness of the authentication mechanism must be ensured for building a secure web application.**
- **Authorization: If the restrictions on what authenticated users are allowed to do are not properly enforced, attackers can exploit the flaws to access other user's accounts, view sensitive files, or use unauthorized functions. Therefore, the authorization of user access must be clearly defined and built in the application.**
- **Error and Exception handling: Error conditions that occur during normal operation should be handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, and cause security mechanisms to fail.**
- **Input validations: The information received by the web applications from the web-requests must be properly validated before being used by a web application. Attackers can tamper the request or part of the request to cause the application to misbehave. Just having very strong input validations can easily prevent many types of attacks.**
- **Session Handling: Attackers that can compromise session cookies and other session related information can defeat authentication restrictions and assume other user's identities. Therefore proper session handling mechanism should be in place.**
- **Encryption and Cryptography: Web applications frequently use cryptographic functions to protect information and credentials. These**

functions and the code to integrate them are difficult to design, and may result in a weak implementation.

- **Physical security: The computer running the web server should be kept physically secured in a locked area. Any backup storage media (tapes, removable disks, etc.) should be similarly protected.**

Key Components of Security

Application Security

Each application will be categorized by the following set of attributes.

- **Type of work (Application Development & Maintenance / Production support)**
- **Availability commitments; i.e. how mission-critical is this application, which in turn will drive the following.**
  - **Distribution of responsibilities between data center and implementation site teams**
  - **Dependence on communication facilities**
  - **Disaster Recovery Strategy for application data (as applicable)**

Affiliations & Standards

- **The keys to sound security are often considered to be: deployment of a sensible security risk analysis approach, compliance with a recognized standard such as ISO 9001:2008, development of comprehensive information security policies and deployment of a detailed security audit program.**

Virus Protection
- **Two tiered approach towards protection from Virus is recommended**
- **Usage of two different anti-virus products ensures that in case any virus escapes any one Antivirus, the other product will take care of that.**
- **Dedicated Infrastructure Development team managing the Anti-virus definition servers.**
- **Daily update of antivirus definitions.**
- **Desktop Antivirus clients and Server configured in classical push pull technology.**
- **Daily Scheduled Scans**
- **Patch management Process is very clearly defined and strictly followed and reviewed**
- **Use of enterprise security manager software to check policy compliance**
- **Use of patch management soft wares**
- **Separate testing environment before deploying patches**
- **Dedicated Infrastructure Team to test, Install and Review the patch management status.**

Performance:

- **The performance of the web based systems is of utmost importance as the users are located at remote locations and connecting through a browser window. The speed of refreshing the data, web pages, uploads and download speed etc has been considered for better performance. A minimum performance standard has to be decided upon and further tuning of both the hardware and software has to be undertaken for better performance.**

Scalability:

- **Since the government business is very dynamic, the scalability issues have to be given due importance. The system architecture defined for SWD (3-tier architecture) helps in scaling of the system horizontally, vertically and diagonally. Horizontal scaling is characterized by rapid application development, but simplified change management. Horizontal scaling can help organizations achieve the right level of resilience. With vertical scaling, services are scaled within the system — resources such as CPUs, memory, and storage can be incrementally added to the server over time to increase scalability. Vertical scaling is characterized by slowly changing applications and is often necessary for data-intensive services such as databases, video servers, mail stores, and directories. Diagonal scaling is a combination of horizontal and vertical scaling. Each server in the group of horizontally scaled servers can be grown within the system, providing increased flexibility.**