

**Request for Proposal  
for  
Selection of Agency for Establishment and Management  
of on premise Security Operation Center (24x7x365 days)  
at Gujarat State Data Center, Gandhinagar,  
DST, Government of Gujarat.**

**Volume-I  
(Commercial Terms and Bid Process)**



**Gujarat Informatics Ltd**  
Block No. 2, 2nd Floor,  
C & D Wing, Karmayogi Bhavan  
Sector - 10 A, Gandhinagar – 382010 Gujarat.  
Ph. No. 23252026, 23258692 Fax: 23238925.

## Abbreviations

- **GoG:** Government of Gujarat
- **DST:** Department of Science & Technology
- **GIL:** Gujarat Informatics Limited
- **GSWAN:** Gujarat State Wide Area Network
- **GSDC:** Gujarat State Data Centre
- **SOC:** Security Operations Center
- **OEM:** Original Equipment Manufacturer
- **O&M:** Operations & Maintenance
- **EMS:** Enterprise Management Suite
- **NMS:** Network Monitoring System
- **EMD:** Earnest Money Deposit
- **PBG:** Performance Bank Guarantee
- **SLA:** Service Level Agreement
- **FAT:** Final Acceptance Test
- **TPA:** Third Party Agency
- **SoW:** Scope of Work
- **SIEM:** Security Information and Event Management
- **SOAR:** Security Orchestration, Automation and Response
- **CCTV:** Closed Circuit Tele Vision
- **QP:** Quarterly Payment
- **TENDERER:** DST/GIL/ Government of Gujarat

## Section I – Invitation for Bids

The invitation to bid is for “Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Centre, Gandhinagar”. The bidders are advised to study the bid document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the bid document with full understanding of its implications. This section provides general information about the Issuer (i.e., Gujarat Informatics Limited), important dates and addresses and the overall eligibility criteria for the bidders.

### 1.1 Issuer

Gujarat Informatics Limited (herein after referred to as “GIL”) a company owned by Department of Science & Technology, Govt. of Gujarat (herein after referred to as “GIL”) invites proposals for Selection of Agency for establishment and management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Centre, Gandhinagar. The scope of work and other requirement of this project are specified in this RFP document.

### 1.2 About The RFP Document

The Request for Proposal (RFP) document consists of two volumes viz.

#### 1.2.1. RFP Volume I – Commercial Terms & Bid Process

- (a) Section I – Invitation for Bids
- (b) Section II – Eligibility Criteria
- (c) Section III – Instructions to Bidders
- (d) Section IV – Terms & Conditions of the Contract
- (e) Section V – Payment Terms
- (f) Section VI – Format for Response to Tender – Pre-Qualification Bid
- (g) Section VII – Format for Response to Tender – Technical Bid
- (h) Section VIII - Format for Response to Tender – Financial Bid
- (i) Annexure 1 – RFP document acknowledgement form
- (j) Annexure 2- Instructions for furnishing Bank Guarantee
- (k) Annexure 3 – Performa of Bank Guarantee towards Performance Security

#### 1.2.2. RFP Volume II – Scope of work and SLAs

- (l) Section I – Introduction
- (m) Section II – Scope of Work
- (n) Section III – Technical Specification
- (o) Section IV – Service Level Agreement (SLAs), Penalties & Payment Terms

### 1.3 Instruction to the bidders for online bid submission

1.4.1. Tender documents are available only in electronic format which Bidders can download free of cost from the website [www.gil.gujarat.gov.in](http://www.gil.gujarat.gov.in) and <https://gem.gov.in/>.

1.4.2. The bids have been invited through e-tendering route i.e., the Pre-qualification, **technical and financial bids shall be submitted online on the website <https://gem.gov.in/>**.

1.4.3. Bidders who wish to participate in this bid will have to register on <https://gem.gov.in/>.

### 1.4 Amendment in RFP Document

At any time before the deadline for submission of bids, GIL may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the

RFP Document by amendment. All the amendments made in the document would be published on the website <https://gil.gujarat.gov.in>. All such amendments shall be binding to all the bidders. **The bidders are also advised to visit the website on regular basis for checking necessary updates.**

**1.5 Address for submission of Bid Security and Correspondence**

All queries and/or correspondence regarding clarification in the bid should be addressed to:

DGM (Tech.), Gujarat Informatics Limited, Block No. 2, 2<sup>nd</sup> Floor, C & D Wing, Karmayogi Bhavan,  
Sector - 10 A, Gandhinagar 382010, Phone: (079)-23252026, 23256033

E-mail: [ddict-gil@gujarat.gov.in](mailto:ddict-gil@gujarat.gov.in); [mgrhn-itcon@gujarat.gov.in](mailto:mgrhn-itcon@gujarat.gov.in)

## Section II – Eligibility Criteria

The bidder must possess the requisite experience, strength and capabilities in providing services necessary to meet the requirements as described in the RFP document. Keeping in view the complexity and volume of the work involved, following criteria are prescribed as the eligibility criteria for the bidder interested in undertaking the project. The bidder must also possess technical know-how and financial wherewithal that would be required to successfully provide required services sought by the State for the entire period of the contract. The Bids must be complete in all respect and should cover entire scope of work as stipulated in the bid document. This invitation to bid is open to all bidders who qualify the eligibility criteria as given below:

| Sr. No. | Criteria   | Documents Required  |
|---------|--|---|
| 1       | The bidder should have annual turnover of at least Rs. <b>50</b> Cr from Information Technology business in India, for last three audited financial years and must have 15 cr. Annual turnover from Information Security/Cyber Security Business in India for any three of last <b>four</b> audited financial years                          | CA certified and audited Balance Sheet and Profit & Loss statement for any three of last <b>four</b> audited financial years (2018-19, 2019-20, 2020-21, 2021-22).<br><br>CA certificate mentioning turnover from the said business.  |
| 2       | The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2021. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC.<br>At least 3 government / BFSI clients.<br>All work orders / contracts should be in the name of the bidder for SOC services.                 | Relevant Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The PO / letter should be in the name of the bidder and clearly mention the scope of work. |
| 3       | The bidder should have minimum manpower strength as per the different skill levels defined in the document:<br>Level 1 analyst – minimum 10.<br>Level 2 analyst – minimum 10.<br>Level 3 analyst - minimum 3.<br>(The manpower criteria as mentioned in the RFP document)<br>All manpower should be on the pay role of the company / bidder. | Certificate from HR head confirming compliance. CVs along with Certifications also required for evaluation purpose.   |

|   |  |   |
|---|--|---|
| 4 | <p>The bidder should have executed assignments within last three years. for Information Security services business, with each project value as follows</p> <ul style="list-style-type: none"> <li>• One project of at least Rs. 10 Crores</li> <li>OR</li> <li>• Two projects of at least Rs 5 crores</li> </ul> <p>Information Security services business is defined as implementing and supporting SOC, implementing Cyber security hardware/software solutions, Hardware/software solution comprises of SIEM/SOAR.</p> <p>Out of the above projects, at least one project should have been implemented in Government/PSU in India assessing Cyber security hardware/cyber security software solutions and providing information security / cyber security services.</p> | <p>Copy of</p> <ol style="list-style-type: none"> <li>1. Work Order</li> <li>2. Agreement (Hiding detailed Commercial Values)</li> <li>3. Work Completion i.e. (Completion of Implementation &amp; Go-Live) Certificate clearly depicting the scope of work, contract period and project value and Client contact details with Mobile number, Landline number and Email ID</li> </ol> |
| 5 | The bidder should not have been blacklisted by Government of India / Government of Gujarat.  | An undertaking to this effect in the company's letter head signed by authorized signatory to be submitted   |
| 6 | The Bidder must have a valid ISO 27001 certificate as on date of publishing of the RFP   | Copy of valid ISO 27001 certificate   |
| 7 | The bidder should have local office in Gujarat or should submit a declaration for establishing an office in Gujarat within 45 days of issuing of PO from tenderer.   | Self-certification with office location addresses to be submitted / declaration for establishment of an office in case PO has been awarded.<br>The document should be on the bidder's letter head signed by the authorized signatory  |
| 8 | The bidder must have positive net worth and should be Profit making in any three of last <b>four</b> audited financial years as on 31st March, 2022  | Audited and Certified Balance Sheet and Profit/Loss Account of last 4 Financial Years should be enclosed. CA certificate mentioning net profit of the bidder should be enclosed.  |

- 1) All details and the supportive documents for the above should be uploaded in the GeM bid.
- 2) Bidder's experience, bidder's turn over criteria, EMD and PBG will not be considered of GeM bid. However, bidder must match eligibility criteria, experience, bidder's turn over criteria, EMD and PBG as mentioned above (in this document) and will be considered for evaluation.  
All bidders who wish to participate in this bid must submit EMD as per bid requirement.

**Technical Evaluation Matrix (Max Marks -100)**

| Sr. No.                          | Technical evaluation criteria   | Document to be submitted  | Marks distribution  |          |
|----------------------------------|---|---|---|----------|
| <b>Company Profile –35 Marks</b> |   |   |   |          |
| 1                                | <p>The bidder should provide the list of clients with whom SOC solution (On premises, Managed, Hybrid) was implemented during last three years up-to 31.03.2021.</p> <p>At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services.</p> <p>Minimum value of any one project should be above 5 crores.</p> | <p>Relevant Work order copy / Client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted.</p> | More than or equal to 6 Govt. / BFSI clients.   | 10 marks |
|                                  |   |   | More than or equal to 4 and less than 6 govt. / BFSI clients.                         | 07 marks |
|                                  |   |   | More than or equal to 2 and less than 4 govt. / BFSI clients.                         | 05 marks |
| 2                                | <p>Experience in implementation of on-premises Cyber Security operations centre.</p>  | <p>Relevant Work order copy / Client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted.</p> | More than or equal to 05 on premises SOC projects implemented successfully / ongoing. | 10 marks |
|                                  |   |   | At least 03 on premises SOC projects implemented successfully / ongoing.              | 07 marks |
|                                  |   |   | At least 02 on-premises SOC projects implemented successfully / ongoing.              | 05 marks |
|                                  | <p>The proposed bidder / OEM has experience</p>   | <p>Relevant MSA copy / Work order copy / Client satisfactory letter</p>   | More than 50000 EPS   | 10 marks |
|                                  |   |   | More than 30000 EPS up to 50000 EPS   | 07 marks |

|                           |  |   |   |          |
|---------------------------|--|---|---|----------|
| 3                         | in implementing at least one project handling 20000 EPS or more  | mentioning the number of EPS and the solution.<br><br>The WO / letter should be in the name of the bidder / OEM and clearly mention the scope of work.  | 20000 EPS up to 30000 EPS   | 05 marks |
| 4                         | Major solutions like SOAR and SIEM should be from OEMs who have both local and global presence, deployed solutions and supported customers globally.   | Declaration from the OEM mentioning the credential details and deployment of solution for customers both within and outside India.  | Yes, have both national and global presence   | 05 marks |
|                           |  |   | No, does not have both national and global presence   | 00 marks |
| <b>Manpower –30 Marks</b> |  |   |   |          |
| 5                         | Certified EC Council-CEH/Comptia Security+/CISSP/CHFI/ Certified SOC Analyst (CSA)-EC Council/ CompTIA CySA+personnel under the payroll of the company | An undertaking in the company's letter head signed by authorized signatory to be submitted.<br><br>The undertaking should mention the name and employee code of the personnel along with certification. | At least 05 CISSP, 05 CHFI, 10 EC Council-CEH/Comptia Security+ and 05 proposed SIEM solution certified personnel and 15 personnel any one certification mentioned. Total 40 personnel. | 10 marks |
|                           |  |   | At least 03 CISSP, 02 CHFI, 5 EC Council-CEH/Comptia Security+ and 05 proposed SIEM solution certified personnel and 10 personnel any one certification mentioned. Total 25 personnel.  | 07 marks |
|                           |  |   | At least 01 CISSP, 02 EC Council-CEH/Comptia Security+ and 03 proposed SIEM solution certified personnel and 9 personnel any one certification mentioned. Total 15 personnel.           | 05 marks |



|                                  |  |   |  |                  |
|----------------------------------|--|---|--|------------------|
| 6                                | Certified resources of proposed team                   | Copies of certificates  | <p>10 marks – 7 or more<br/>EC Council-CEH/Comptia Security+/CISSP/CHFI/Certified SOC Analyst (CSA)-<br/>EC Council/ CompTIA CySA+ certified professionals allocated</p> <p>7 marks – 5 or more<br/>EC Council-CEH/Comptia Security+/CISSP/CHFI/Certified SOC Analyst (CSA)-<br/>EC Council/ CompTIA CySA+ certified professionals allocated</p> <p>5 marks – 5 or more<br/>EC Council-CEH/Comptia Security+/CISSP/CHFI/Certified SOC Analyst (CSA)-<br/>EC Council/ CompTIA CySA+ certified professionals allocated</p> <p>2 marks – 4<br/>EC Council-CEH/Comptia Security+/CISSP/CHFI/Certified SOC Analyst (CSA)-<br/>EC Council/ CompTIA CySA+ certified professionals allocated</p> | Maximum 10 marks |
| 7                                | Quality of resources to be proposed for SOC operations | The quality / scoring of resources would be considered through CV scrutiny to be held through a technical panel of SOC/DST. | <p>CV scrutiny of resource proposed for Level 3 analyst – Max 3 marks</p> <p>CV scrutiny of resources proposed for Level 2 analyst - 1 marks for each resource</p> <p>CV scrutiny of resources proposed for Level 1 analyst - 1 marks for each resource</p>  | Maximum 10 marks |
| Technical Presentation –35 Marks |  |   |  |                  |

|   |  |   |   |          |
|---|--|---|---|----------|
| 8 | Quality of technical design, approach methodology, solution specifications | Technical presentation to be given by the bidder to SOC/DST.                      | Marks would be distributed as per the approach and methodology, past experiences and credentials presented by the bidder.             | 15 marks |
| 9 |  | Marks would be awarded as per the technical committee of evaluation from SOC/DST. | Marks would be awarded as per superiority in terms of technical specifications & capacity of the solutions as proposed by the bidder. | 20 marks |

Passing mark should be 70

### Section III - Instruction to Bidders

#### 3.1 Bidding Documents

- 3.1.1 Bidder can download the bid document and further amendment if any freely available on <https://gil.gujarat.gov.in> and <https://gem.gov.in/> and upload their response/proposal on <https://gem.gov.in/> on or before due date of the tender.
- 3.1.2 Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents thoroughly. Failure to furnish all information required as per RFP or submission of a Bid not substantially responsive to the RFP in every respect may result in the rejection of the Bid.
- 3.1.3 Under no circumstances physical bid will be accepted.

#### 3.2 Clarification on Bidding Documents

- 3.2.1 A prospective Bidder requiring any clarification of the bidding documents may seek clarifications by submitting queries on email Id: [ddict-gil@gujarat.gov.in](mailto:ddict-gil@gujarat.gov.in); prior to the date of Pre Bid Meeting.
- 3.2.2 Tenderer will discuss the queries received from the interested bidders in the Pre Bid Meeting and respond the clarifications by uploading on the website <https://gil.gujarat.gov.in>.
- 3.2.3 No further or new clarification whatsoever shall be entertained after the Pre Bid Meeting.
- 3.2.4 The interested bidder should send the queries as per the following format:

| Bidder's Request For Clarification      |   |   |   |
|---|---|---|---|
| Name of Organization submitting request |   | Name & position of person submitting request: | Address of organization including phone, fax, email points of contact |
| S.No.                                   | Bidding Document Reference (Clause /page) | Content of RFP requiring clarification        | Points of Clarification required                                      |
| 1                                       |   |   |   |
| 2                                       |   |   |   |
| 3                                       |   |   |   |
| 4                                       |   |   |   |

### 3.3 Amendments to RFP

- 3.3.1 At any time prior to the deadline for submission of bids, TENDERER, for any reason, whether on its own initiative or in response to the clarifications requested by prospective bidders, may modify the bidding documents by amendment and publish corrigendum on the websites <https://gil.gujarat.gov.in> and <https://gem.gov.in/>.
- 3.3.2 All prospective bidders are requested to check above mentioned websites, any amendments/corrigendum/modification will be notified on these websites and such modification will be binding on them.
- 3.3.3 In order to allow prospective bidders a reasonable time to take the amendment into Account in preparing their bids, TENDERER, at its discretion, may extend the deadline for the submission of bids.

### 3.4 Language of Bid

- 3.4.1 The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and TENDERER shall be in English.
- 3.4.2 In case, supporting documents and printed literature furnished by the bidder is in some other language, accurate translation of the relevant pages in English would be required. For the purpose of interpretation of the bid, the translation in English shall govern.

### 3.5 Documents Comprising the Bid

- 3.5.1 The Bid prepared by the Bidder shall comprise of the following documents:
- (a) **Bid Security/EMD and Bid Processing Fee:** The Bidder shall furnish, as part of the Bid, a Bid security for the amount of **Rs. 50,00,000/- (Rs. Fifty lac) EMD** in the form of Demand Draft OR in the form of an unconditional Bank Guarantee (which should be valid for **9 months from the last date of bid submission**) of any Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative Banks and Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the **G.R. no. EMD/10/2021/7729/DMO dated 12.04.2021** issued by Finance Department or further instruction issued by Finance department time to time; in the name of "Gujarat Informatics Ltd." payable at Gandhinagar (as per prescribed format and must be submitted along with the covering letter.
- (b) **Pre-qualification Bid:** In support of eligibility, a bidder must submit the following documents:
- (i) Volume I, Section VI – Format 1: Pre-qualification Bid Letter.
  - (ii) Volume I, Section VI – Format 2: General information about the Bidder.
  - (iii) Detailed checklist for Eligibility dully filled in along with the supporting documents as defined in Volume I, Section VI – Format 3
  - (iv) Declaration that the bidder has not been blacklisted by any Ministry of Government of India or by Government of any State in India or by Government of Gujarat or any of the Government PSUs as per Volume I, Section VI – Format 4. – Declaration Regarding Blacklisting

- (v) Undertaking by the bidder for acceptance to the Terms & Conditions mentioned in this RFP, Section VI- Format 5: Undertaking for Acceptance of Terms and Conditions in RFP.
  - (vi) Annual turnover as per Eligibility criteria Sr. no. 1 and 8, Section VI – Format 6: Annual Sales Turnover Statement
  - (vii) Experience of projects of prescribed nature and size as per Eligibility Criteria Sr. no. 2 and 4 - Format 7: Completion of Projects of Prescribed Nature and Size
- (c) **Technical Bid:** The Technical Bid besides the other requirements of the RFP, shall comprise:
- (i) Volume I, Section VII– Format 1: Technical Bid Letter
  - (ii) Volume I, Section VII – Format 2: Technical Compliance Sheet
  - (iii) Volume I, Section VII – Format 3: Relationship with OEM
  - (iv) Volume I, Section VII – Format 4: Proposed Technical Solution
  - (v) Volume I, Section VII – Format 5: Project Management Plan
  - (vi) Volume I, Section VII – Format 6: Core Project Team
- (d) **Financial Bid:** The Financial Bid, besides the other requirements of the RFP, shall comprise of the following:
- (i) Volume I, Section VIII – Format 1: Financial Bid Letter
  - (ii) Volume I, Section VIII –Format-2: Price Bid

3.5.2 The Pre-qualification Bid, Technical Bid and Financial Bid must be submitted online through the e-tendering website of <https://gem.gov.in/> online portal.

### 3.6 Bid Forms

3.6.1 Wherever a specific form is prescribed in the Bid document, the Bidder shall use the form to provide relevant information. If the form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information. Failing to upload the information in the prescribed format, the bid is liable for rejection.

3.6.2 For all other cases, the Bidder shall design a form to hold the required information.

3.6.3 TENDERER shall not be bound by any printed conditions or provisions in the Bidder's Bid Forms.

### 3.7 Fraudulent and Corrupt Practice

3.7.1 Fraudulent practice means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the TENDERER of the benefits of free and open competition.

- 3.7.2 “Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official in the process of Contract execution.
- 3.7.3 TENDERER will reject a proposal for award and may forfeit the EMD and/or Performance Bank Guarantee if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing, contract(s).

### **3.8 Local / Site Conditions**

- 3.8.1 It will be incumbent upon each Bidder to fully acquaint itself with the local conditions and other relevant factors for SOC at GSDC Gandhinagar which would have any effect on the performance of the contract and / or the cost. The Bidders are advised to visit the GSDC Gandhinagar locations (at their own cost) and due-diligence should be conducted before the pre-bid meeting/ bid-submission.
- 3.8.2 The Bidder is expected to make a site visit to obtain for itself all information that may be necessary for preparing the bid and entering into contract.
- 3.8.3 Failure to obtain the information necessary for preparing the bid and/or failure to perform activities that may be necessary for providing the services before entering into contract will in no way relieve the Successful Bidder from performing any work in accordance with the RFP documents.
- 3.8.4 It will be imperative for each Bidder to fully inform themselves of all legal conditions and factors which may have any effect on the execution of the contract as described in the RFP Documents. TENDERER shall not entertain any request for clarification from the Bidder regarding such conditions.
- 3.8.5 It is the responsibility of the Bidder that such factors have properly been investigated and considered while submitting the bid proposals and that no claim whatsoever including those for financial adjustment to the contract awarded under the RFP Documents will be entertained by TENDERER and that neither any change in the time schedule of the contract nor any financial adjustments arising thereof shall be permitted by TENDERER on account of failure of the Bidder to appraise themselves of local laws and site conditions.

### **3.9 Lack of Information to Bidder**

The Bidder shall be deemed to have carefully examined all RFP documents to its entire satisfaction. Any lack of information shall not in any way relieve the Bidder of its responsibility to fulfil its obligation under the Contract.

### **3.10 Contract Obligations**

If after the award of the contract the Bidder does not sign the contract or fails to furnish the Performance Bank Guarantee (PBG) within fifteen working days from the date of award and if

the operations are not started within 70 working days after submission of Kickoff date, TENDERER reserves the right to cancel the contract and apply all remedies available under the terms and conditions of this contract.

### **3.11 Bid Price**

- 3.11.1 The Price/Financial bid should indicate the prices in the format/price schedule only.
- 3.11.2 Offered prices should be exclusive of GST inclusive of levies such as Excise, Insurance, FOR destination (anywhere in the Gujarat state).
- 3.11.3 Discount if offered, should not be mentioned separately. It should be included in offered price.
- 3.11.4 Prices shall be written in both words and figures. In the event of difference, the price in words shall be valid and binding.
- 3.11.5 The unit rate should be quoted against each line item listed in the respective Annexures attached in this bid. Quantities can be increased or decreased by TENDERER and bidder has to supply deviated quantities at the rates prescribed and approved by TENDERER in the tender document.
- 3.11.6 If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If the Bidder does not accept the correction of the errors, its bid will be rejected.
- 3.11.7 Any discrepancy relating to prices quoted in the offer across different sections of the bid, only prices given in the prescribed format given at Price Schedule of this RFP shall prevail.
- 3.11.8 The quoted prices shall be valid for 365 days from the date of opening of financial bid.
- 3.11.9 The Bidder has to submit detailed breakup of each financial price bid as per the attached Financial annexure for SOC in separate sealed cover and should be submitted at the time of bid submission. As GEM is not allowing breakup of so many items, detailed breakup is to be submitted in physical sealed cover. Physical sealed cover would be opened in front of eligible participants at the time of financial bid opening. Rates submitted on GEM portal of all the aggregated cost under the Schedule -I and Schedule-II of the price schedule will only be considered for L1 Evaluation. The physical price bid submitted to GIL for price breakup will be used during contract period for any addition / deletion of the item under the scope.
- 3.11.10 RA has been enabled in the GEM Bid. The discount offered in RA by the successful bidder will be applicable in the physical price breakup and price bid submitted by bidder at GIL office.

### **3.12 Bid Currency**

Prices shall be quoted in Indian rupees only.

**3.13 Period of Validity of Bids**

3.13.1 Bids shall remain valid for 180 days from the date of Financial Bid opening. A Bid valid for a shorter period shall be rejected as non-responsive.

3.13.2 In exceptional circumstances, TENDERER may solicit Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The Bid security shall also be suitably extended. A Bidder's request to modify the Bid will not be permitted.

**3.14 Bid Due Date**

3.14.1 Bid must be submitted on the e-tendering website <https://gem.gov.in/> not later than the date/time specified in the RFP.

3.14.2 The TENDERER may, at its discretion, extend the bid due date, in which case all rights and obligations of the TENDERER and the bidders, previously subject to the bid due date, shall thereafter be subject to the new bid due date as extended.

**3.15 Late Bid**

Bidders would not be able to upload or submit the bid after the bid due date/time.

**3.16 Modification and Withdrawal of Bid**

3.16.1 The Bidder may modify or withdraw its Bid before the due date of bid submission on e-tendering website <https://gem.gov.in/>.

3.16.2 No Bid may be modified subsequent to the deadline for submission of bids.

3.16.3 No Bid may be withdrawn after due date for submission of bids. Withdrawal of a Bid after Bid submission due date may result in the forfeiture of bidder's Bid security.

**3.17 Opening of Bids by TENDERER**

3.17.1 Bids will be opened in the presence of Bidder's representatives, who choose to attend. The Bidder's representatives who are present shall sign a register evidencing their attendance.

3.17.2 The Bidder's names, Bid modifications or withdrawals, discounts and the presence or absence of relevant Bid security and such other details as the TENDERER at its discretion, may consider appropriate, will be announced at the opening.

3.17.3 Immediately after the closing time, the TENDERER shall open the Pre-qualification Bids and list them for further evaluation.

**3.18 Contacting TENDERER**

3.18.1 Bidder shall not approach TENDERER officers outside of office hours and/ or outside TENDERER office premises, from the time of the Bid opening to the time the Contract is awarded.



3.18.2 Any effort by a bidder to influence TENDERER officers in the decisions on Bid evaluation, bid comparison or contract award may result in rejection of the Bidder's offer. If the Bidder wishes to bring additional information to the notice of the TENDERER, it should do so in writing.

### **3.19 Rejection Criteria**

3.19.1 Besides other conditions and terms highlighted in the RFP document, bids may be rejected under the following circumstances:

#### **a) Pre-qualification Rejection Criteria**

- (i) Bids submitted without or with improper Bid Security (EMD) and Bid Processing fee.
- (ii) Bids which do not conform to unconditional validity of the bid as prescribed in the bid.
- (iii) If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the Tendering Process.
- (iv) Any effort on the part of a Bidder to influence the bid evaluation, bid comparison or contract award decisions.
- (v) Bids without proper documents/evidence as asked for in the pre-qualification bid as mentioned in the RFP Document.

#### **b) Technical Rejection Criteria**

- (i) Technical Bid containing financial details.
- (ii) Revelation of Prices in any form or by any reason before opening the Financial Bid.
- (iii) Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the Bid Document in every respect.
- (iv) Bidders not quoting for the complete scope of Work as indicated in the Bid documents, addendum (if any) and any subsequent information given to the Bidder.
- (v) Bidders not complying with the Technical and General Terms and conditions as stated in the RFP Documents.
- (vi) Bidders not conforming to unconditional acceptance of full responsibility of providing services in accordance with the Scope of work and Service Level Agreements of this RFP.
- (vii) If the bid does not confirm to the timelines indicated in the RFP Document.

#### **c) Financial Rejection Criteria**

- (i) Incomplete Price Bid
- (ii) Price Bids that do not conform to the Bid's price bid format.

### **3.2 Rejection of Bids**

TENDERER reserves the right to reject any Bid, and to annul the bidding process and reject all

bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidders or any obligation to inform the affected Bidders of the grounds for such decision.

### **3.3 Evaluation Methodology**

- 3.3.1 TENDERER will form a Committee which will evaluate the proposals submitted by the bidders for a detailed scrutiny. During evaluation of proposals, TENDERER, may, at its discretion, ask the bidders for clarification of their Proposals.
- 3.3.2 The Pre-qualification Bids will be evaluated first to ascertain the eligibility of the Bidders.
- 3.3.3 The technical bids of the bidders who comply with the eligibility criteria in the Pre-qualification Bids will be opened. The technical evaluation would be based on the technical presentation and proposal of Bidder meeting the Specifications mentioned in the RFP document and other compliance to the terms and conditions. In case of conditional bid or major deviations from the RFP requirements, TENDERER may seek the clarification in writing from the bidder, if required. If bidder fails to submit the required clarifications in due time, the technical evaluation will be done based on the information submitted in the technical bid.
- 3.3.4 The Financial Bids of Technically qualified bidders only would be opened and evaluated to determine the L1 bidder. **The Criteria for selection will be the lowest cost to the TENDERER i.e., Sum total of all the line items without taxes for the qualified bid.** TENDERER/GIL may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.
- 3.3.5 Bidder is allowed to quote only one make & model for each line item. Further, bidders are not allowed to change the quoted make & model during the contract period

### **3.4 Award of Contract**

- 3.4.1 Award Criteria: The Criteria for selection will be the lowest cost to TENDERER amongst the technically qualified bids.
- 3.4.2 TENDERER's right to vary requirements at time of award: TENDERER reserves the right at the time of award to increase or decrease quantity for the requirements originally specified in the document without any change in Bid rate or other terms and conditions.
- 3.4.3 In case, if lowest bidder does not accept the award of contract or found to be involved in corrupt and/or fraudulent practices, the next lowest bidder will be awarded the contract, if he agrees to match the price quoted by L1/Lowest bidder.

### **3.5 Notification of Award and Signing of Contract**

- 3.5.1 Prior to expiration of the period of Bid validity, TENDERER will notify the successful Bidders and issue Lol.
- 3.5.2 The successful bidder has to submit the Performance Bank Guarantee (PBG) within fifteen (15) working days of receipt of award. The PBG should be 10% of total contract value and valid up to 180 days beyond the expiry of the contract.

### **3.6 Contract Obligations and Amendment to Contract**

- 3.6.1 Once a contract is confirmed and signed, the terms and conditions contained therein shall take precedence over the Bidder's bid and all previous correspondence.
- 3.6.2 Amendments to the Contract may be made by mutual agreement by both the Parties.
- 3.6.3 No variation in or modification in the terms of the contract shall be made except by written amendment signed by both the parties. All alterations and changes in the contract will take into account prevailing rules, regulations and laws applicable in the State of Gujarat.

### **3.7 Use of Contract Documents and Information**

- 3.7.1 The bidder shall not without prior written consent from TENDERER disclose the Contract or any provision thereof or any specification, plans, drawings, pattern, samples or information furnished by or on behalf of GoG in connection therewith to any person other than the person employed by the Vendor in the performance of the Agreement. Disclosure to any such employee shall be made in confidence and shall extend only as far as may be necessary for such performance.
- 3.7.2 The bidder shall not without prior written consent of TENDERER make use of any document or information made available for the project except for purposes of performing the Contract.
- 3.7.3 All project related documents issued by TENDERER other than the Contract itself shall remain the property of TENDERER and Originals and all copies shall be returned to TENDERER on completion of the bidder's performance under the Contract, if so required by the TENDERER.

### **3.8 Confidentiality of the Document**

- 3.8.1 This Bid Document as submitted by the bidder would be treated as confidential and TENDERER shall ensure that anything contained in this Bid Document shall not be disclosed in any manner, whatsoever to any party/unrelated person to the Bid process.

## Section IV - General Conditions of the Contract

### 4.1 Application

These general conditions shall apply to the extent that they are not superseded by provisions in other parts of the contract. For interpretation of any clause in the RFP or Contract Agreement, the interpretation of the TENDERER shall be final and binding on the agency.

### 4.2 Standard

The selected agency shall give the services and carry out their obligations under the Contract with due diligence, efficiency and economy in accordance with generally accepted professional standards and practices. The selected agency shall always act in respect of any matter relating to this contract as faithful advisor to TENDERER. The selected agency shall abide by all the provisions/Acts/Rules etc. of Information Technology prevalent in the country as on the date of the requirements and design submissions. The equipments and services supplied under this contract shall conform to the standards mentioned in the requirement specifications.

### 4.3 Patent Rights

The selected agency shall indemnify TENDERER against all third party claims of infringement of patent, trademark or industrial design rights arising from the use of the equipments and services or any part thereof.

### 4.4 Incidental Services

The Selected agency may be required to provide any or all of the following services:

4.4.1 Furnish detailed manuals for each appropriate unit of the supplied equipment and services.

4.4.2 Perform or supervise or maintain and/ or repair the supplied equipment and services, for a period of time agreed by TENDERER and the selected agency, provided this service shall not relieve the Selected agency of any warranty obligations under this contract.

### 4.5 Delivery and Documents

The selected agency shall submit all the deliverables on due date as per the delivery schedule agreed between parties. No party shall, without the other party's prior written consent, disclose contract, drawings, specifications, plan or other documents to any person other than an entity employed by the affected party for the performance of the contract. In case of the termination of the contact, all the documents prepared by the selected agency under this contract shall become the exclusive property of TENDERER. The Selected agency may retain a copy of such documents, but shall not use anywhere, without taking permission, in writing, from TENDERER. TENDERER reserves right to grant or deny such permission. Delivery of the equipments and services and associated documents shall be made by the selected agency in accordance with the terms specified by TENDERER in RFP.

### 4.6 Change Orders

4.6.1 TENDERER may at any time, by a written order given to the Selected agency make changes within the general scope of the contract in any one or more of the following:

- (a) Configuration or specifications of the equipment.
- (b) The service to be provided by the Selected agency.

#### **4.7 Assignment**

The Selected agency shall not assign, in whole or in part, his obligations to perform under the contract, to any other party or persons, except with TENDERER's prior written consent. The permission, if any, of TENDERER has to be taken before award of the contract.

#### **4.8 Sub Contract**

The Selected agency would provide the services on its own and no back-to-back sub-contracting shall be allowed. However, if sub-contracting for specialized work is required, the Selected agency will take prior permission from TENDERER.

#### **4.9 Take Over**

TENDERER or any agency authorized by TENDERER has the right to take over the operations and management SOC even before the expiry of 5 years in case the successful bidder fails to perform any obligations under the contract.

#### **4.10 Inappropriate use of Network**

The Selected agency shall not use the network facilities/ equipment installed for any other purpose/ use than that of the functions assigned by the TENDERER.

#### **4.11 Termination for Default**

DST/ GoG may, without prejudice to any other remedy for breach of contract can terminate the contract, in whole or in part after giving 30 days prior written notice of default sent to the Selected agency:

4.11.1 If the Selected agency fails to deliver any or all of the equipments and services within the time periods specified in the contract, or any extension thereof granted by DST/ GIL  
OR

4.11.2 If the Selected agency fails to perform any obligations under the contract

#### **4.12 Termination for Insolvency**

4.12.1 TENDERER may at any time terminate the contract by giving 30 days prior written notice to the Selected agency, without compensation to the Selected agency, if the Selected agency 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 TENDERER.

4.12.2 In the event of termination as per clause above (4.11 & 4.12), TENDERER reserves the right to take suitable action against successful bidder against their default including revoking the PBG and risk purchase clause etc.

#### **4.13 Force Majeure**

- 4.13.1 The Selected agency shall not be liable for forfeiture of his performance security, liquidated damages or termination for default, if and to the extent that, his delay in performance or other failure to perform his obligations under the contract is the result of an event of Force Majeure.
- 4.13.2 For purposes of this clause, "Force Majeure" means an event beyond the control of the Selected agency and not involving the Selected agency and not involving the Selected agency's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of DST/ GoG either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
- 4.13.3 If a Force Majeure situation arises, the selected agency shall promptly notify DST/ GoG in writing of such conditions and the cause thereof. Unless otherwise directed by DST/ GoG, the selected agency shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- 4.13.4 **Force Majeure Events:** The Force Majeure circumstances and events shall include the following events to the extent that such events or their consequences (it being understood that if a causing event is within the reasonable control of the affected party, the direct consequences shall also be deemed to be within such party's reasonable control) satisfy the definition as stated above.
- 4.13.5 Without limitation to the generality of the foregoing, Force Majeure Event shall include following events and circumstances and their effects to the extent that they, or their effects, satisfy the above requirements:
- (a) **Natural events** ("Natural Events") to the extent they satisfy the foregoing requirements including:
- (i) Any material effect on the natural elements, including lightning, fire, earthquake, cyclone, flood, storm, tornado, or typhoon;
  - (ii) Explosion or chemical contamination (other than resulting from an act of war);
  - (iii) Epidemic such as plague, covid-19 etc.;
  - (iv) Any event or circumstance of a nature analogous to any of the foregoing.
- (b) **Political Events** which occur inside or Outside the State of Gujarat or directly involve the State Government and the Central Government ("Direct Political Event"), including:
- (i) Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act of terrorism or sabotage;
  - (ii) Strikes, work to rules, go-slows which are either widespread, nation- wide, or state-wide or are of political nature;

(iii) Any event or circumstance of a nature analogous to any of the foregoing

#### 4.13.6 Force Majeure Exclusions

(a) Force Majeure shall not include the following event(s) and/or circumstances, except to the extent that they are consequences of an event of Force Majeure:

(i) Unavailability, late delivery

(ii) Delay in the performance of any contractor, sub-contractors or their agents;

4.13.7 **Procedure for Calling Force Majeure:** The Affected Party shall notify to the other Party in writing of the occurrence of the Force Majeure as soon as reasonably practicable, and in any event within five days after the affected Party came to know or ought reasonably to have known, of its occurrence and that the Force Majeure would be likely to have a material impact on the performance of its obligations under the contract.

4.13.8 **Payments in case of Force Majeure:** During the period of their inability of services as a result of an event of Force Majeure, the Selected agency shall be entitled to continue to be paid under the terms of this contract, as well as to be reimbursed for costs additional costs reasonably and necessarily incurred by them during such period purposes for the purpose of the services and in reactivating the service after the end of such period.

#### 4.14 Resolution of Disputes

4.14.1 If any dispute arises between parties, then there would be two ways for resolution of the dispute under the Contract.

(a) **Amicable Settlement:** Performance of the contract is governed by the terms the conditions of the contract, however at times dispute may arise about any interpretation of any term or condition of contract including the Schedule of Requirement, the clauses of payments etc. In such a situation dispute arising between parties are out of contract, either party of the contract may send a written notice of dispute to the other party. The party receiving the notice of dispute will consider the notice and respond to it in writing within 30 days after receipt. If that party fails to respond within 30 days, or the dispute cannot be amicably settled within 60 days following the response of that party, then 'Arbitration' clause shall become applicable. Amicable settlement clause shall be only applicable in case of dispute is arising out of contract. The said clause shall not be applicable in the case of cyber-crimes and any other type of security breach carried out by either bidder organization itself or its employees.

(b) **Arbitration:** In the case dispute arising between the parties in the contract, which has not been settled amicably, any party can refer the dispute for Arbitration under (Indian) Arbitration and Conciliation Act, 1996. Such disputes shall be referred to Arbitral Tribunal as prescribed by Ministry of Law, Government of India. The Indian Arbitration and Conciliation Act, 1996 and any statutory modification or reenactment thereof, shall apply to these arbitration

proceedings.

4.14.2 Arbitration proceedings will be held in India at Gandhinagar and the language of the arbitration proceeding and that of all documents and communications between the parties shall be in English.

4.14.3 The decision of the majority of arbitrators shall be final and binding upon both the parties.

4.14.4 All arbitration awards shall be in writing and shall state the reasons for the award.

4.14.5 The expenses of the arbitration as determined by the arbitrators shall be shared equally between the two parties. However, the expenses incurred by each party in connection with the preparation, presentation shall be borne by the party itself.

4.14.6 Arbitration clause shall be only applicable in case of dispute is arising out of contract. The said clause shall not be applicable in the case of cyber-crimes and any other type of confidentiality/security breach carried out by either bidder organization itself or its employees.

4.14.7 Both the parties agree the jurisdiction of Adjudicating Authority, Gujarat state and Cyber Appellate Tribunal, New Delhi under Information Technology Act, 2000 (including any amendments therein) in case of any contraventions, security and confidentiality breaches.

#### **4.15 Governing Language**

The contract shall be written in English. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in the same language.

#### **4.16 Applicable Law**

Applicable Law means the laws and any other instruments having the force of law in India as they may be issued and in force from time to time. The contracts shall be interpreted in accordance with the laws of the Union of India and that of the State of Gujarat.

#### **4.17 Notices**

Any notice by one party to the other pursuant to the contract shall be sent in writing by registered post only to the addresses as defined under this contract. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

#### **4.18 Back up support**

Selected agency shall furnish details of the back-up engineering and network support that will be available to TENDERER. If the maintenance of the equipment, after expiry of the contract period, is taken over either by TENDERER or any other person/ agency to be nominated by TENDERER, the Selected agency shall be responsible for provisioning of spare parts and back-up maintenance support required by TENDERER or that agency and shall continue to make available the spare parts.

#### **4.19 Statutory Deductions and Payment**

4.19.1 Payments shall be subject to any deductions (such as TDS, penalty as per SLAs, etc.) of any amount, for which the Selected agency is liable under the agreement against this RFP.



4.19.2 The payments to the Selected agency will be made quarterly at the end of each quarter on Acceptance of the invoice by the TENDERER or its designated agency. The invoice would be processed for release of payment within 45 days after due verification of the invoice and other supporting documents by TENDERER or its designated agency. However, in case the processing of the invoice gets delayed beyond 45 days from the date of acceptance of invoice, the Selected agency would be paid an ad-hoc amount of 50% of invoice value and the remaining amount would be released after getting clarifications, due verification and imposition of penalty, if any.

#### **4.20 Taxes and Duties**

The Selected agency shall fully familiarize itself about the applicable Domestic taxes (such as GST, Income Tax, duties, fees, levies, etc.) on amount payable by TENDERER under the contract. The Selected agency shall pay such domestic tax, duties, fees and other impositions (wherever applicable) levied under the applicable law. The billing should be done in Gujarat only.

#### **4.21 Insurance**

The equipments covered under this contract (as per Annexures enclosed with this RFP) shall be fully insured by the selected agency against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation. The selected agency will have to procure insurance for all the assets under SOC on behalf of TENDERER within six months from the date of kick-off meeting. TENDERER shall provide authorization to the selected agency to procure insurance.

#### **4.22 Manuals, Data and Information**

Complete information relating to installation, maintenance, service, support, and troubleshooting of equipments and services should be supplied by the selected agency.

#### **4.23 Inspection and Testing (in case of replacement/new procurement, suggested by bidder as part of solution)**

4.23.1 The bidder will have to offer the inspection after delivering and installing the equipments at the SOC.

4.23.2 Any deviation found in the specification of the delivered equipments after inspection from the tender specifications will lead to the cancellation of the order, forfeiture of PBG and prohibition in the participation in the future purchases of Government of Gujarat.

4.23.2 The TENDERER's right to inspect, test and, where necessary, reject the Goods after the Goods arrival at Customer Sites shall in no way be limited or waived by reason of the

Goods having previously been inspected, tested and passed by the Purchaser or its representative prior to the Goods shipment.

4.23.3 DST may appoint Third Party Agency, who would monitor the project during implementation, commissioning and operation. The Third-Party Agency will also conduct the Partial and Final Acceptance Test as per the technical requirement of the Agreement. Third Party Agency will verify the services provided by the Bidder under the Agreement. The successful bidder will co-operate with such Third-Party Agency.

4.23.4 In case, if bidder wish to have support from any external agency, it's very necessary to inform DST in written prior to allow them to work on DST/GOG infrastructure. The information should contain all respective information about the company from whom support has been extended, the person/group of people and the segment in which services has been taken. On completion of the task, another report should be submitted mentioning action taken by this person/group of people from external agency, with duration. The bidder is sole responsible for the action taken by such agency on their behalf. No Data/ Information should be sent out of the premise without obtaining prior written confirmation from the DST.

#### **4.24 Limitation of Liability**

Selected agency's cumulative liability for its obligations under the contract shall not exceed the contract value and the selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.

#### **4.25 Confidentiality**

4.25.1 Selected agency understands and agrees that all materials and information marked and identified by TENDERER as 'Confidential' are valuable assets of TENDERER and are to be considered TENDERER's proprietary information and property. Selected agency will treat all confidential materials and information provided by TENDERER with the highest degree of care necessary to ensure that unauthorized disclosure does not occur. Selected agency will not use or disclose any materials or information provided by TENDERER without TENDERER's prior written approval.

4.25.2 Selected agency shall not be liable for disclosure or use of any materials or information provided by TENDERER or developed by Selected agency which is:

- (a) possessed by Selected agency prior to receipt from TENDERER, other than through prior disclosure by TENDERER, as documented by Selected agency's written records;
- (b) published or available to the general public otherwise than through a breach of Confidentiality; or
- (c) Obtained by Selected agency from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to TENDERER; or
- (d) Developed independently by the selected agency.

4.25.3 In the event that selected agency is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, Selected agency shall promptly notify TENDERER and allow TENDERER a reasonable

time to oppose such process before making disclosure.

- 4.25.4 Selected agency understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause DST, GoG irreparable harm, may leave TENDERER with no adequate remedy at law and TENDERER is entitled to seek to injunctive relief.
- 4.25.5 TENDERER does not wish to receive the Confidential Information of Selected agency, and selected agency agrees that it will first provide or disclose information which is not confidential. Only to the extent that TENDERER requests Confidential Information from Selected agency, then selected agency will furnish or disclose Confidential Information.
- 4.25.6 Nothing herein shall be construed as granting to either party any right or license under any copyrights, inventions, or patents now or hereafter owned or controlled by the other party. The requirements of use and confidentiality set forth herein shall survive the expiration, termination or cancellation of this RFP. Confidential Information disclosed under this contract shall be subject to confidentiality obligations for a period of two years following the initial date of disclosure. Nothing contained in this contract shall limit the selected agency from providing similar services to any third parties or reusing the skills, know-how, and experience gained by the employees in providing the services contemplated under this contract.

#### **4.26 Use of Contract document and Information**

- 4.26.1 The selected agency shall not, without TENDERER's prior written consent, disclose the contract or any provision thereof, or any specification, design, drawing, pattern, sample or information furnished by or on behalf of TENDERER in connection therewith, to any person other than a person employed by the Selected agency in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
- 4.26.2 The Selected agency shall not without TENDERER's prior written consent, make use of any Document or information forming a part of this RFP except for purpose of performing the contract. Any document forming a part of this RFP, other than the contract itself, shall remain the property of TENDERER

#### **4.27 Severability**

If any term, clause or provision of the agreement shall be judged to be invalid for any reason whatsoever such invalidity shall not affect the validity or operation of any other term, clause or provision of the agreement and such invalid term clause or provision shall be deemed to have been deleted from the agreement and if the invalid portion is such that the remainder cannot be sustained without it, both parties shall enter into discussions to find a suitable replacement to the clause that shall be legally valid.

#### **4.28 Contract Period**

The contract shall remain valid for a period of five years from the date of FAT and end with the date of completion of five years of service. However, TENDERER reserves a right to terminate the contract by sending a notice to the bidder in the events of non-performance, security

violations and non-compliance.

#### **4.29 Performance Bank Guarantee of the Contract**

4.29.1 The Performance Bank Guarantee (PBG) has to be submitted within fifteen (15) working days of receipt of award. The PBG should be 10% of total contract value and valid up to 180 days beyond the expiry of contract.

4.29.2 The PBG shall be denominated in Indian Rupees and shall be in the form of a Bank Guarantee Bond from of all Nationalized Bank including the public sector bank or Private Sector Banks authorized by RBI or Commercial Bank or Regional Rural Banks of Gujarat or Co-Operative Bank of Gujarat (operating in India having branch at Ahmedabad/ Gandhinagar) as per the [G.R. No. EMD/10/2021/7729/DMO dated 12.04.2021 issued by Finance Department](#) and further GR issued by FD time to time. (in the Performa given in this document)

4.29.3 The Performance Guarantee shall be discharged by GoG and returned to the Service Provider within 30 days from the date of expiry of the Performance Bank Guarantee.

#### **4.30 Successful bidder (Selected agency's) Obligations**

The Selected agency would be required to maintain and manage (including integration of new equipment/replaced equipment as a part of this bid) the SOC facilities. It will be the selected agency's responsibility to ensure compliance to the requirements of the SOC and continued operations of the SOC in accordance with and in strict adherence to the terms of the RFP and the Contract.

4.30.1 In addition to the aforementioned, the Selected agency shall:

- (a) Perform the Services specified by TENDERER and make available the necessary equipment / facilities / services as may be necessary and 'Scope of work' requirements as specified in the bid and changes thereof.
- (b) The Selected agency shall ensure that its team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. The Selected agency shall ensure that the Services are performed in accordance with the terms hereof and to the satisfaction of TENDERER. Nothing in this Contract relieves the Selected agency from its liabilities or obligations under this Contract to provide the Services in accordance with TENDERER directions and requirements as stated in the Contract and the Bid to the extent accepted by TENDERER and the Selected agency shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its team.
- (c) The Selected agency's representatives shall have all the powers requisite for the performance of services under this contract. The Selected agency's representatives shall liaise with TENDERER's representatives for the proper coordination and timely completion of the works and on any other matters pertaining to the works. The Selected agency will extend full co-operation to TENDERER's representatives in

the manner required by them for supervision / inspection / observation of the SOC facilities, equipment / material, procedures, performance, reports and records pertaining to the works. Selected agency shall also have complete charge of the selected agency's personnel engaged in the performance of the works and to ensure internal discipline, compliance of rules, regulations and safety practices. Selected agency shall also co-ordinate and co-operate with the other Service Providers / Vendors of TENDERER working at the site/offsite for activities related to planning, execution of scope of work and providing services under this contract.

#### 4.30.2 Reporting Progress:

- (a) The Selected agency shall monitor progress of all the activities specified in the contract and submit monthly progress report about various aspects of the work to TENDERER as per Scope of Work. TENDERER on mutual agreement between both parties may change the periodicity of such reports. Extracts of the progress report to be termed, as "Executive Summary" shall be submitted in 3 copies, along with 3 copies of monthly progress report. The same is required to be submitted in soft copy as well. Formats for such reporting shall be discussed at the Kick-off meeting.
- (b) The SOC facilities / services and / or Labour to be provided by the selected agency under the Contract and the manner and speed of execution and maintenance of the work are to be conducted in a manner to the satisfaction of TENDERER in accordance with the Contract. The rate of progress of the work compliance to the requirements of the SOC or their facilities or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works or insufficient for satisfactory operations of the SOC, TENDERER shall so notify the Selected agency in writing.
- (c) The Selected agency shall reply to the written notice giving details of the measures they propose to take to expedite the progress so as to complete the works by the prescribed time. The Selected agency shall not be entitled to any additional payment for taking such steps. If at any time it should appear to TENDERER that the actual progress of work does not conform to the approved plan the Selected agency shall produce at the request of TENDERER a revised plan showing the modification to the approved plan necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance/improvement to the stipulated requirements.

#### 4.30.3 Knowledge of Site Conditions:

- (a) The Selected agency's undertaking of this Contract shall be deemed to mean that the selected agency possesses the knowledge of requirements as stipulated in the RFP.
- (b) The Selected agency shall be deemed to have understood the requirements and have satisfied itself with the data contained in the RFP Document, the quantities and nature of the works and materials necessary for the completion of the works, etc. and in-general to have obtained itself all necessary information of all risks, contingencies and circumstances affecting its obligations and responsibilities therewith under the Contract and its ability to perform it.

- (c) Selected agency shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price for the works. The consideration provided in the Contract for the Selected agency undertaking the works shall cover all the Selected agency's obligation and all matters and things necessary for proper execution and maintenance of the works in accordance with the Contract and for complying with any instructions which TENDERER may issue in accordance with the connection therewith and of any proper and reasonable measures which the Selected agency takes in the absence of specific instructions from TENDERER.

#### **4.31 Selected agency's Team**

- 4.31.1 The Selected agency shall supply to TENDERER manpower not less than the proposal made in the proposed technical solution of the RFP, to be established by the selected agency for execution of the work / facilities including the identities and Curriculum-Vitae of the key personnel to be deployed during Kick-off meeting.
- 4.31.2 The selected agency shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and for all costs / charges in connection thereof.
- 4.31.3 The Selected agency shall provide and deploy manpower on the Site for carrying out the work, only those manpower resources who are skilled and experienced in their respective trades and who are competent to execute or manage / supervise the work in a proper and timely manner as per the RFP.
- 4.31.4 TENDERER may at any time object to and require the Selected agency to remove forthwith from the site an employee of the Selected agency or any persons deployed by Selected agency, if in the opinion of TENDERER, the person in question has misconducted himself or his deployment is otherwise considered undesirable by TENDERER, the Selected agency shall forthwith remove and shall not again deploy the person in question of the work site without the written consent of TENDERER.
- 4.31.5 TENDERER may at any time request the Selected agency to remove from the work / Site the selected agency's supervisor or any other authorized representative including any employee of the selected agency, or any person(s) deployed by selected agency for professional incompetence or negligence or for being deployed for work for which he is not suited. The selected agency shall consider the request and may accede to or disregard it. TENDERER having made a request as aforesaid in the case of any person which the Selected agency has disregarded, may in the case of the same person at any time but on a different occasion and for a different instance of one of the reasons referred to above in this Clause object to and require the Selected agency to remove that person from deployment on the work which the Selected agency shall then forthwith do and shall not again deploy any person so objected to on the work or on the sort of work in question (as the case may be) without the written consent of TENDERER.
- 4.31.6 TENDERER shall state to the Selected agency in writing its reasons for any request or requirement pursuant to this clause.
- 4.31.7 The selected agency shall maintain backup personnel for each domain which should be screened through DST and shall promptly provide replacement of every person

removed pursuant to this section with an equally competent substitute from the pool of backup personnel. The resume should be screened in advance and same resources should be made available as replacement.

- 4.31.8 In case of change in its team composition owing to attrition the selected agency shall ensure a reasonable amount of time-overlap in activities to ensure proper knowledge transfer and handover/takeover of documents and other relevant materials between the outgoing and the new member.
- 4.31.9 The entire scope of the work depends on the technical skill and experience in management of the same level or kind of SOC infrastructure.
- 4.31.10 It is mandatory for successful bidder to deploy qualified professional to install, commission and maintain the equipments, as defined under scope of work.
- 4.31.11 The successful bidder has to submit regular schedule of manpower availability and get it approved by DST.
- 4.31.12 The successful bidder has to deploy necessary problem escalation process and system to take care users at priority.
- 4.31.13 The successful bidder is free to deploy or to develop applications to facilitate the operation. DST will welcome the deployment such application in respect to improve Quality of Services.
- 4.31.14 For extending better services to the government, the successful bidder will be allowed to deploy and use own tested and proven solution, with prior permission form the DST.
- 4.31.15 The successful bidder needs to manage and maintain various records related to the services extended to the Government.
- 4.31.16 The successful bidder is responsible to maintain documentation on the progress of the work and will have to update the same on regular basis. Bidder will have to submit the progress reports regularly, as per the guideline issued by DST.
- 4.31.17 The escalation of any rate during the rate contract is not permitted.
- 4.31.18 The Selected agency will be responsible to carry out on job training mentioned below but not limited to, on quarterly basis and submit the content of training, attendance, and output / result of the training. Technical skill development, soft skill development, Quality & Safety training.

#### **4.32 Statutory Requirements**

- 4.32.1 During the tenure of this Contract nothing shall be done by the selected agency in contravention of any law, act and / or rules / regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep TENDERER indemnified in this regard.
- 4.32.2 The selected agency and their personnel/representative shall not alter / change / replace any hardware component proprietary to TENDERER and / or under warranty or AMC of third party without prior consent of TENDERER.
- 4.32.3 The selected agency and their personnel/representative shall not without consent of TENDERER install any hardware or software not purchased / owned by TENDERER.

#### **4.33 Contract Administration**

- 4.33.1 Either party may appoint any individual / organization as their authorized representative through a written notice to the other party. Each representative shall have the authority to:

- (i) Exercise all of the powers and functions of his / her Party under this Contract other than the power to amend this Contract and ensure the proper administration and performance of the terms hereof and
  - (ii) Bind his or her Party in relation to any matter arising out of or in connection with this Contract.
- 4.33.2 The selected agency along with the members of sub-contracted agency / third party shall be bound by all undertakings and representations made by the authorized representative of the Selected agency and any covenants stipulated hereunder with respect to this Contract for and on their behalf.
- 4.33.3 For the purpose of execution or performance of the obligations under this Contract TENDERER's Representative would act as an interface with the nominated representative of the selected agency. Selected agency shall comply with any instructions that are given by TENDERER's Representative during the course of this Contract in relation to the performance of its obligations under the terms of this Contract and the RFP.
- 4.33.4 A Committee comprising of representatives from TENDERER and the selected agency shall meet on a mutually agreed time or weekly basis to discuss any issues / bottlenecks being encountered. The Selected agency shall draw the minutes of these meetings and circulate to TENDERER.

#### **4.34 Right of Monitoring, Inspection and Periodic Audit**

- 4.34.1 TENDERER reserves the right to inspect and monitor / assess the progress / performance / management of the SOC facilities at any time during the course of the Contract, after providing due notice to the Selected agency. TENDERER may demand and upon such demand being made TENDERER shall be provided with any document, data, material or any other information which it may require to assess the progress of the project/ delivery of services.
- 4.34.2 TENDERER shall also have the right to conduct, either itself or through another third party as it may deem fit, an audit to monitor the performance of the Selected agency of its obligations / functions in accordance with the standards committed to or required by TENDERER and the Selected agency undertakes to cooperate with and provide to TENDERER / any other third party appointed by TENDERER, all documents and other details as may be required by them for this purpose. Any deviations or contravention identified as a result of such audit/assessment would need to be rectified by the selected agency failing which TENDERER may without prejudice to any other rights that it may have issued a notice of default.

#### **4.35 Information Security**

- 4.35.1 The Selected agency shall not carry and / or transmit any material, information, layouts, diagrams, storage media or any other goods / material in physical or electronic form, which are proprietary to or owned by TENDERER, without prior written permission from TENDERER.
- 4.35.2 The Selected agency shall adhere to the Information Security policy developed by TENDERER.



4.35.3 Selected agency acknowledges that TENDERER business data and other TENDERER proprietary information or materials, whether developed by TENDERER or being used by TENDERER pursuant to a license agreement with a third party (the foregoing collectively referred to herein as “proprietary information”) are confidential and proprietary to TENDERER and Selected agency agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Selected agency to protect its own proprietary information. Selected agency recognizes that the goodwill of TENDERER depends, among other things, upon selected agency keeping such proprietary information confidential and that unauthorized disclosure of the same by Selected agency could damage TENDERER and that by reason of Implementation Agency’s duties hereunder. Selected agency may come into possession of such proprietary information even though Selected agency does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. Selected agency shall use such information only for the purpose of performing the said services.

4.35.4 Selected agency shall, upon termination of this agreement for any reason or upon demand by TENDERER, whichever is earlier return any and all information provided to Selected agency by TENDERER including any copies or reproductions, both hard copy and electronic.

#### **4.36 Relationship between the Parties**

4.36.1 Nothing in this Contract constitutes any fiduciary relationship between TENDERER and Selected agency’s Team or any relationship of employer employee, principal and agent, or partnership, between TENDERER and Selected agency.

4.36.2 No Party has any authority to bind the other Party in any manner whatsoever except as agreed under the terms of this Contract.

4.36.3 TENDERER has no obligations to the Selected agency’s Team except as agreed under the terms of this Contract.

#### **4.37 Special Terms and Conditions**

4.37.1 Secondhand Equipment: Any proposed equipments shall be new and no secondhand equipment shall be accepted. Occurrence of such an event, will amount to mischief and fraudulence and the Bidder shall be liable for penal action.

4.37.2 Acceptance Test: A Testing Committee shall be constituted comprising of officers duly authorized by TENDERER and/or any third-party agency appointed by it. The acceptance tests shall be carried at each site by the committee.

#### **4.38 Final Acceptance Test (FAT)**

4.38.1 The Equipment shall be deemed to be commissioned, subject to successful FAT. Availability of all the defined services shall be verified. The Selected agency shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP for each site.

4.38.2 All documentation as defined should be completed before the final acceptance test.

- 4.38.3 On successful completion of the final acceptance and TENDERER are satisfied with the working of the system, the acceptance certificate signed by TENDERER will be issued to the selected agency.
- 4.38.4 The date on which final acceptance certificate is issued shall be deemed to be date of successful commission of the equipment. Any delay by the selected agency in commissioning of equipments shall render the selected agency liable to the imposition of appropriate liquidated damages.

#### **4.39 SLA Monitoring**

- 4.39.1 TENDERER may engage third party audit agency or designate any agency/team for SLA management and monitoring. This third-party audit agency shall monitor the SLA parameters and generate reports on regular basis. TENDERER reserves the right to periodically change the measurement points and methodologies used.
- 4.39.2 The Selected agency shall use an Enterprise/Network Management System for monitoring and measurement of the SLA parameters prescribed for SOC.

#### **4.40 Exit Management**

##### **4.40.1 Purpose**

- (a) This clause sets out the provisions which will apply upon completion of the contract period or upon termination of the agreement for any reasons. The Parties shall ensure that their respective associated entities, in case of TENDERER, any third party appointed by TENDERER and in case of the selected agency, carry out their respective obligations set out in this Exit Management Clause.
- (b) The exit management period starts 3 months before the expiry of contract or in case of termination of contract, the date on which the notice of termination is sent to the selected agency.
- (c) The exit management period ends on the date agreed upon by TENDERER or one year after the beginning of the exit management period, whichever is earlier.
- (d) The Parties shall ensure that their respective associated entities, authorized representative of or its nominated agencies and the vendor carry out their respective obligations set out in this Exit Management Clause.
- (e) Before the expiry of the exit management period, the Selected agency shall deliver to TENDERER or its nominated agencies all new or up-dated materials from the categories set out in point 4.5 above, and shall not retain any copies thereof, except that the Selected agency shall be permitted to retain one copy of such materials for archival purposes only.
- (f) After completion of contract period (5 years), the contract may be extended next two year subject to the service of the selected agency and TENDERER's discretion.

##### **4.40.2 Cooperation and Provision of Information**

- (a) During the exit management period:
  - (i) The Selected agency will allow TENDERER or any third party appointed by

- TENDERER, access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable TENDERER or any third party appointed by TENDERER to assess the existing services being delivered;
- (ii) Promptly on reasonable request by TENDERER or any third party appointed by TENDERER, the selected agency shall provide access to, and copies of all information held or controlled by them which they have prepared or maintained in accordance with the "Contract", the Project Plan, SLA and Scope of Work, relating to any material aspect of the services. TENDERER or any third party appointed by TENDERER shall be entitled to copy all such information. Such information shall include details pertaining to the services rendered and other performance data. The Selected agency shall permit TENDERER, or any third party appointed by TENDERER to have reasonable access to its employees and facilities as reasonably required by TENDERER or any third party appointed by TENDERER to understand the methods of delivery of the services employed by the Selected agency and to assist appropriate knowledge transfer.
  - (iii) Before the end of exit management period, the Selected agency will ensure a successful trial run of SOC equipments, tools, software, etc. by TENDERER or by any third party appointed by TENDERER.
- (b) Confidential Information, Security and Data
- (i) The selected agency will promptly, on the commencement of the exit management period, supply to TENDERER or any third party appointed by TENDERER the following:
    - a. Information relating to the current services rendered and performance data in relation to the services.
    - b. Documentation related to Intellectual Property Rights.
    - c. All confidential information related to TENDERER.
    - d. All current and updated TENDERER data as is reasonably required by TENDERER or any third party appointed by TENDERER for purposes of transitioning the services to TENDERER or any third party appointed by TENDERER, in a format prescribed by TENDERER or any third party appointed by TENDERER.
    - e. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable TENDERER or any third party appointed by TENDERER, to carry out due diligence in order to transition the provision of the Services to TENDERER or any third party appointed by TENDERER, (as the case may be).
  - (ii) Before the expiry of the exit management period, the Selected agency shall deliver to TENDERER, or any third party appointed by TENDERER all new or updated materials from the categories set out above and shall not retain any copies thereof.
  - (iii) Before the expiry of the exit management period, unless otherwise provided

under the "Contract", TENDERER or any third party appointed by TENDERER shall deliver to the selected agency all forms of "Selected agency's" confidential information which is in the possession or control of TENDERER or any third party appointed by TENDERER.

- (c) Right of Access to Premises
  - (i) At any time during the exit management period, where Assets are located at the Selected agency's premises, the selected agency will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) TENDERER or any third party appointed by TENDERER in order to take stock of the Assets.
  - (ii) The selected agency shall also give TENDERER, or any third party appointed by TENDERER, right of reasonable access to its premises and shall procure TENDERER or any third party appointed by TENDERER, rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the "Contract" as is reasonably necessary to migrate the services to TENDERER or any third party appointed by TENDERER.
- (d) General Obligations of the Selected agency
  - (i) The Selected agency shall provide all such information as may reasonably be necessary to bring into effect seamless handover as practicable in the circumstances to TENDERER or any third party appointed by TENDERER and which the selected agency has in its possession or control at any time during the exit management period.
  - (ii) For the purposes of this Clause, anything in the possession or control of any selected agency or associated entity is deemed to be in the possession or control of the selected agency.
  - (iii) The Selected agency shall commit adequate resources to comply with its obligations under this Exit Management Clause.

#### 4.40.3 Exit Management Plan

The selected agency shall provide TENDERER, or any third party appointed by TENDERER with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the "Contract" as a whole and in relation to the Project Plan, SLA and Scope of Work.

- (a) A detailed program of the transfer process that could be used in conjunction with TENDERER or any third party appointed by TENDERER including details of the means to be used to ensure continuing provision of the services throughout the transfer process and of the management structure to be used during the transfer.
- (b) Plans for the communication with such of the Selected agency's staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on TENDERER's operations as a result of undertaking the transfer.
- (c) Identification of specific security tasks necessary at termination.
- (d) Plans for provision of contingent support to TENDERER or any third party appointed

by TENDERER for a reasonable period after transfer for the purposes of seamlessly replacing the Services.

- 4.40.4 The Selected agency shall re-draft the Exit Management Plan annually to ensure that it is kept relevant and up to date.
- 4.40.5 Each Exit Management Plan shall be presented by the selected agency to and approved by TENDERER or any third party appointed by TENDERER.
- 4.40.6 In case of expiry or termination of contract, each Party shall comply with the Exit Management Plan.
- 4.40.7 During the exit management period, the selected agency shall deliver services as per contract.
- 4.40.8 Payments during the Exit Management period shall be made in accordance with the Terms of Payment Clause.
- 4.40.9 This Exit Management plan shall be furnished in writing to TENDERER or any third party appointed by TENDERER within 90 days from the Effective Date of "Contract".

#### **4.41 Representations and warranties**

##### **4.41.1 Representations and Warranties by the selected agency**

- (a) It is a company/ organization under any statute of India duly organized and validly existing under the laws of India and has all requisite legal power and authority and corporate authorizations to execute the Agreement and carry out the terms, conditions and provisions hereof;
- (b) It has in full force and effect all requisite clearances, approvals and permits necessary to enter into the Agreement and perform its obligations hereof;
- (c) It will have the legally valid and enforceable title to all Equipment as may be necessary for proper functioning and it will be free from all encumbrances, liens, charges, any security interest and adverse claims of any description;
- (d) The Agreement and the transactions and obligations hereof do not contravene its constitutional documents or any law, regulation or government directive and will not contravene any provisions of, or constitute a default under, any other Agreement or instrument to which it is a party or by which it or its property may be bound or any of its obligations or undertakings by which it or any of its assets are bound or cause a limitation on its powers or cause it to exceed its authorized powers;
- (e) Necessary approvals/ clearances concerned authorities, for establishing the proposed project are to be obtained by the successful bidder.
- (f) Necessary approvals/ clearances from concerned authorities, as required, for fire protection, government duties / taxes / Octroi, are to be obtained by the successful bidder.
- (g) Necessary approvals/ clearances, from concerned authorities (like City Nagar, Nigam, Public Works Department (PWD), Department of Irrigation, State Electricity Board etc.), as required, are to be obtained by the successful bidder to meet system requirements.
- (h) There is no pending or threatened actions, suits or proceedings affecting the Selected agency or its affiliates or any of their respective assets before a court,

governmental agency, commission or arbitrator or administrative tribunal which affects the Selected agency's ability to perform its obligations under the Agreement; and neither Selected agency nor any of its affiliates have immunity from the jurisdiction of a court or from legal process (whether through service of notice, attachment prior to judgment, attachment in aid of execution or otherwise);

- (i) The Selected agency confirms that all representations and warranties of the selected agency set forth in the Agreement are true, complete and correct in all respects;
- (j) No information given by the selected agency in relation to the Agreement, project documents or any document comprising security contains any material misstatement of fact or omits to state as fact which would be materially adverse to the enforcement of the rights and remedies of TENDERER or which would be necessary to make any statement, representation or warranty contained herein or therein true and correct;
- (k) All equipment including material to be installed by the selected agency in the SOC shall be new. All equipment shall conform to the codes, standards and regulations applicable to networking facilities and benefit from the usual manufacturer's guarantees.

#### 4.41.2 Representations and Warranties by TENDERER

- (a) It has full legal right; power and authority to execute the SOC and to enter into and perform its obligations under the Agreement and there are no proceedings pending.
- (b) The Agreement has been duly authorized, executed and delivered by TENDERER and constitutes valid, legal and binding obligation of TENDERER.
- (c) The execution and delivery of the Agreement with the selected agency does not violate any statutory judgment, order, decree, regulation, right, obligation or rule of any court, government authority or arbitrator of competent jurisdiction applicable in relation to TENDERER, its assets or its administration.

#### 4.42 Each Day during the Agreement

The Parties agree that these representations and warranties are taken to be made on each Day during the term of the Agreement.

#### 4.43 Indemnity

Successful Bidder will defend and/or settle any claims against TENDERER that allege that Bidder branded product or service as supplied under this contract infringes the intellectual property rights of a third party. Successful Bidder will rely on Customer's prompt notification of the claim and cooperation with our defense. Bidder may modify the product or service so as to be non-infringing and materially equivalent, or TENDERER may procure a license. If these options are not available, TENDERER will refund to Customer the amount paid for the affected product in the first year or the depreciated value thereafter or, for support services, the balance of any pre-paid amount or, for professional services, the amount paid. Bidder is not responsible for claims resulting from any unauthorized use of the products or services. This section shall also apply to deliverables identified as such in the relevant Support Material except that Bidder is not responsible for claims resulting from deliverables content or design provided by Customer.

**4.44 Risk Purchase**

TENDERER on identifying any material breach of contract by Bidder, shall give Bidder a cure period of 60 days to correct the breach. If Bidder fails to cure the breach in the said time duration and accept its inability to correct, TENDERER may terminate the part of the contract that is breached and employ a third party to do the work on behalf of TENDERER. Bidder shall not be liable for any compensation for the work executed this way. Bidder shall execute the balance part of work as agreed under the contract.

## Section V – Payment Terms

### 5.1 Payment Schedule

| S/N                         | Activity   | Payment (%)  |
|-----------------------------|--|--|
| <b>Table 1: Schedule-I</b>  |  |  |
| 1                           | Delivery of all components (Hardware, Software, Licenses, etc.) at SOC, Gandhinagar  | 70% of the sum total of schedule I of financial bid  |
| 2                           | Successful installation, Testing, Integration, Commissioning   | 10% of the sum total of schedule I of financial bid  |
| 3                           | Successful completion of training & Final Acceptance test of entire solution   | 20% of the sum total of schedule I of financial bid  |
| <b>Table 2: Schedule-II</b> |  |  |
| 1                           | 5 Years AMC/warranty/O&M and Back to Back OEM support and operation costs including manpower for the entire Infrastructure | Will be divided and paid in 20 equal Quarterly Installments after the end of each quarter (3 months). Five years will start from the date of successfully completion of FAT. |



**Section VI– Formats to Response to the RFP: Pre-qualification Bid****6.1 Format 1: Pre-Qualification Bid Letter**

To,

**DGM(Technical)**

Gujarat Informatics Limited

8th Floor, Block -1, Udyog Bhavan, Sector - 11,

Gandhinagar 382010, Gujarat, India

Sir/Madam,

Sub: Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat.

**Reference: RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

We, the undersigned Bidder, having read and examined in detail the entire Bid documents do hereby propose to provide the services as specified in the above referred Bid document number along with the following:

1. **Earnest Money Deposit (EMD):** We have enclosed an EMD in the form of a Demand Draft/ Bank Guarantee no. \_\_\_\_\_ dated xx/xx/xxxx for Rs. 50,00,000/- (Rupees Fifty lacs only) drawn on \_\_\_\_\_. This EMD is liable to be forfeited in accordance with the provisions of this RFP.
2. **Contract Performance Bank Guarantee:** We hereby declare that in case the contract is awarded to us, we shall submit the contract performance bank guarantee in the form prescribed in Volume I, Annexure 3 - Proforma and as per Section IV - General Conditions of Contract.
3. We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.
4. We understand that our bid is binding on us and that you are not bound to accept a bid you receive.

Thankingyou,

Yours faithfully,

(Signature of the Bidder)  
 Printed Name Designation  
 Seal Date:  
 Business Address:

**6.2 Format 2: General Information about the Bidder**

| Details of the Bidder |   |       |       |        |
|-----------------------|---|-------|-------|--------|
| 1.                    | Name of the Bidder & Address of the Bidder  |       |       |        |
| 2.                    | Status of the Company (Public Ltd/ Pvt. Ltd)  |       |       |        |
| 3.                    | Details of Incorporation of the Company   |       |       | Date:  |
|                       |   |       |       | Ref. # |
| 4.                    | Details of Commencement of Business   |       |       | Date:  |
|                       |   |       |       | Ref. # |
| 5.                    | Company Identification Number (CIN)   |       |       |        |
| 6.                    | Registered Office of the Company :  |       |       |        |
| 7.                    | Composition of the Board of Directors of the Company. Please furnish Name, Designation and their DIN. |       |       |        |
| 8.                    | Name of Company Secretary of the Company and his/her Membership No.                                   |       |       |        |
| 9.                    | Name and address of the Statutory Auditors of Company for the Financial years                         |       |       |        |
| 10.                   | Valid GST registration No. & Date   |       |       |        |
| 11.                   | Permanent Account Number (PAN)  |       |       |        |
| 12.                   | Name & Designation of the contact person to whom all references shall be made regarding this tender   |       |       |        |
| 13.                   | Telephone No. (with STD Code)   |       |       |        |
| 14.                   | E-Mail of the contact person:   |       |       |        |
| 15.                   | Fax No. (with STD Code)   |       |       |        |
| 16.                   | Website   |       |       |        |
| 17.                   | Financial Details (as per audited Balance Sheets) (in Cr)   |       |       |        |
|                       | Year  | Year1 | Year2 | Year3  |
|                       | Net Worth   |       |       |        |
|                       | Total Turnover  |       |       |        |
|                       | PAT   |       |       |        |

**6.3 Format 3: Pre-qualification Checklist**

| Sr. No. | Eligibility Criteria   | Attachments  | Supporting Document Uploaded Yes/No |
|---------|--|--|-------------------------------------|
| 1       | <p>The bidder should have annual turnover of at least Rs. <b>50</b> Cr from Information Technology business in India, for last three audited financial years and must have 15 cr. Annual turnover from Information Security/Cyber Security Business in India for any three of last <b>four</b> audited financial years</p>   | <p>CA certified and audited Balance Sheet and Profit &amp; Loss statement for any three of last <b>four</b> financial years (2018-19, 2019-20, 2020-21, 2021-22).</p> <p>CA certificate mentioning turnover from the said business.</p>  |                                     |
| 2       | <p>The bidder should provide the list of clients with whom SOC solution was implemented during last three years up-to 30.12.2021. SOC solution could be On-premises SOC, Managed SOC, Hybrid SOC.</p> <p>At least 3 government / BFSI clients. All work orders / contracts should be in the name of the bidder for SOC services.</p>                               | <p>Relevant Work order copy / client satisfactory letter regarding successful implementation or ongoing of security operation centre (SOC) solution in the name of the bidder is to be submitted. The PO / letter should be in the name of the bidder and clearly mention the scope of work.</p> |                                     |
| 3       | <p>The bidder should have minimum manpower strength as per the different skill levels defined in the document:</p> <p>Level 1 analyst – minimum 10.<br/>Level 2 analyst – minimum 10.<br/>Level 3 analyst - minimum 3.<br/>(The manpower criteria as mentioned in the the RFP document)</p> <p>All manpower should be on the pay role of the company / bidder.</p> | <p>Certificate from HR head confirming compliance. CVs along with Certifications also required for evaluation purpose.</p>   |                                     |

|   |  |   |  |
|---|--|---|--|
| 4 | <p>The bidder should have executed assignments within last three years. for Information Security services business, with each project value as follows</p> <ul style="list-style-type: none"> <li>• One project of at least Rs. 10 Crores</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• Two projects of at least Rs 5 crores</li> </ul> <p>Information Security services business is defined as implementing and supporting SOC, implementing Cyber security hardware/software solutions, Hardware/software solution comprises of SIEM/SOAR. Out of the above projects, at least one project should have been implemented in Government/PSU in India assessing Cyber security hardware/cyber security software solutions and providing information security / cyber security services.</p> | <p>Copy of</p> <ol style="list-style-type: none"> <li>1. Work Order</li> <li>2. Agreement (Hiding detailed Commercial Values)</li> <li>3. Work Completion i.e. (Completion of Implementation &amp; Go-Live) Certificate clearly depicting the scope of work, contract period and project value and Client contact details with Mobile number, Landline number and Email ID</li> </ol> |  |
| 5 | <p>The bidder should not have been blacklisted by Government of India / Government of Gujarat.</p>   | <p>An undertaking to this effect in the company's letter head signed by authorized signatory to be submitted</p>  |  |
| 6 | <p>The Bidder must have a valid ISO 27001 certificate as on date of publishing of the RFP</p>  | <p>Copy of valid ISO 27001 certificate</p>  |  |
| 7 | <p>The bidder should have local office in Gujarat or should submit a declaration for establishing an office in Gujarat within 45 days of issuing of PO from tenderer.</p>  | <p>Self-certification with office location addresses to be submitted / declaration for establishment of an office in case PO has been awarded. The document should be on the bidder's letter head signed by the authorized signatory</p>  |  |
| 8 | <p>The bidder must have positive net worth and should be Profit making in any three of last four audited financial years as on 31st March, 2022</p>  | <p>Audited and Certified Balance Sheet and Profit/Loss Account of last 4 Financial Years should be enclosed. CA certificate mentioning net profit of the bidder should be enclosed.</p>   |  |

#### 6.4 Format 4: Technical Bid Format.

##### Note:

The bidder has to upload/attach/submit a file as per below format along with relevant brochures mentioning the item quoted, its make and model and Deviation/ Remarks (if any) as per specifications mentioned in Volume II

| S/N | Item Description | Unit | Make and Model | Matched/ Not Matched | Remarks If any | Brochures/ Supporting Document Attached (Yes/No) |
|-----|------------------|------|----------------|----------------------|----------------|--|
|-----|------------------|------|----------------|----------------------|----------------|--|

|          |  |  |  |  |  |  |
|----------|--|--|--|--|--|--|
| <b>1</b> |  |  |  |  |  |  |
| <b>2</b> |  |  |  |  |  |  |
| <b>3</b> |  |  |  |  |  |  |
| <b>4</b> |  |  |  |  |  |  |
| <b>5</b> |  |  |  |  |  |  |

Note: For manpower, kindly attach CV and certificates

Important Note: Immediate temporary Replacement of faulty equipment/s need to be provided to end-users during the period of repair without any additional cost to Govt. of Gujarat. Bidder is required to maintain sufficient spare inventory for the above purpose.

6.5 Format 5: Format for MAF / OEM Authorization.

Format of MAF/OEM Authorization

No. \_\_\_\_\_ dated \_\_\_\_\_

To  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Ref: Tender No. \_\_\_\_\_

Subject: \_\_\_\_\_

Dear Sir,

We, \_\_\_\_\_ who are established and reputed manufacturers of \_\_\_\_\_ having factories at \_\_\_\_\_ (address of factory) do hereby authorize M/s. \_\_\_\_\_ (Name & Address of agent) to submit a bid, and sign the contract with you against above mentioned tender No:

We authorized the \_\_\_\_\_ (name of the bidder) for the following modules/products:

| Sr. No. | Product Name | Make & Model |
|---------|--------------|--------------|
|         |              |              |
|         |              |              |

We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s \_\_\_\_\_ (SI/Bidder).

Yours faithfully,

(Name)  
(Name of manufacturers)

### 6.6 Format 6: Declaration Regarding Blacklisting

To,

**DGM(Technical)**

Gujarat Informatics Limited  
Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No \_\_\_\_\_] regarding Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat. I hereby declare that my company has not been blacklisted by any Ministry of Government of India or by Government of any State in India or by Government of Gujarat or any of the Government PSUs. I further certify that I am the Director/Company Secretary and am therefore, competent in my Company to make this declaration.

Yours faithfully,

(Signature of the Bidder) Printed Name

Designation

Seal DIN/Membership No.

Date: Business Address:

**6.7 Format 7: Undertaking for Acceptance of Terms and Conditions in RFP**

To,

**DGM (Technical)**

Gujarat Informatics Limited

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,

Sector 10A, Gandhinagar, Gujarat 382010

Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No. \_\_\_\_\_] regarding Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat. I declare that all the terms and conditions and provisions of this RFP Document including SoW and SLAs are acceptable to my company. I further certify that I am the Director/Company Secretary and am therefore, competent in my Company to make this declaration.

Yours faithfully,

(Signature of the Bidder)

Printed Name Designation

Seal DIN/Membership No. Date:

Business Address:



**6.8 Format 8: Annual Sales Turnover Statement**  
(On Applicant's Statutory Auditor's letterhead)

Date:

This is to certify that we M/s \_\_\_\_\_ are the statutory Auditors of M/s \_\_\_\_\_ and that the below mentioned calculations are true as per the Audited Financial Statements of M/s \_\_\_\_\_ for the below mentioned years. (any three out of 4 FY)

| Sr. | Turnover   | 2018-2019 | 2019-2020 | 2020-2021 | 2021-2022 |
|-----|--|-----------|-----------|-----------|-----------|
| 1   | Annual Turnover as per Profit and Loss Account                                       |           |           |           |           |
| 2   | Net worth as per Audited Balance Sheet   |           |           |           |           |
| 3   | Turnover generated solely from Information Security/Cyber Security Business in India |           |           |           |           |
| 4   | Net Profit as per Profit & Loss Account  |           |           |           |           |

Yours faithfully,

(Signature of the Auditor) Printed Name

Designation

Seal DIN/Membership No. Date:

Business Address:

**Note:** Please upload the Copy of the audited Annual Accounts of the company for the last three years including Balance sheet, Profit & Loss A/c, Directors' Report and Statuary Auditor's Report.

**6.9 Format 9: Completion of Projects of Prescribed Nature and Size**

(Please fill one separate form for each project according to pre-qualification criteria.)

| S. No. | Criteria  | Project   |
|--------|---|---|
| 1      | Implementer Company   |   |
| 2      | Customer's Name   |   |
| 3      | Scope of the Project  | Please provide scope of the project, highlight Key Result Areas expected and achieved |
| 4      | Value of Project  |   |
| 5      | Did the project involve implementation and/or maintenance of On-premises SOC, Managed SOC, Hybrid SOC | Yes/No  |
| 6      | No. of Devices monitored  |   |
| 7      | Completion certificate  | Yes/No  |
| 9      | Customer Contact Person's detail  |   |
| A      | Name  |   |
| B      | Designation   |   |
| C      | Email   |   |
| D      | Phone   |   |
| E      | Fax   |   |
| F      | Mailing address   |   |

- Note: 1. The Copies of work order and the client certificates for satisfactory completion of the project and showing the order value and cost.
2. Completion certificate of prescribed nature and size as mentioned to be uploaded.

## Section VII – Format for Response to RFP: Technical Bid

### 7.1 Format 1: Technical Bid Letter

To,

**DGM (Technical)**

Gujarat Informatics Limited

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Sir/Madam,

Sub: Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat

**Reference: RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

We, the undersigned Bidder, having read and examined in detail the entire Bid documents do hereby propose to provide the services as specified in the above referred Bid document number along with the following:

1. We declare that all the services shall be performed strictly in accordance with the bid documents. Further we agree that additional conditions or assumptions, if any, found in the RFP documents shall not be given effect to.
2. We agree to abide by this bid for a period of 180 days from the date of financial bid opening or for any further period for which bid validity is extended and it shall remain binding upon us and Bid may be accepted at any time before the expiration of that period.
3. We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.
4. We understand that our bid is binding on us and that you are not bound to accept a bid you receive.

Thanking you,

Yours faithfully,

(Signature of the Bidder)  
Printed Name Designation  
Seal Date:  
Business Address:

## 7.2 Format 2: Relationship with OEM

Bidder needs to enclose the authorization on OEM's letterhead for direct OEM support for major critical equipments like SIEM, SOAR, Video-Wall, any other hardware/software but not limited to including existing assets covered in this Contract. During the contract period, if OEM declares any equipment as end of support for any reasons, OEM has to replace that equipment with better or equivalent products without any cost to GoG. OEM has to also submit on their letter head, complete details on the support available for the equipment, their end of support dates and replacement model if any. Format enclosed.

### Format for Certificate of Support from OEM

To  
DGM (Technical)  
Gujarat Informatics Limited  
Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Dated:

**Subject: Support for "Name of OEM" Inventory installed and in use for GSDC**

**Reference: RFP No: <Bid Ref. NUMBER> Dated <DD/MM/YYYY>**

Certified the hardware / software mentioned in Annexure A, for which our company, "**Name of OEM**" is the OEM, has been quoted for support in the bid of M/s. (Partner name)

Subject to existence of valid pre-purchased support contract with "Name of OEM" we undertake to provide the following:

1. TAC Support for operation, maintenance and upgrade of the quoted product on 24 x 7 basis up to 31<sup>st</sup> Dec 2027.
2. RMA replacement when required identified and approved by "Name of OEM" Technical Team (with an equivalent or upgrade model)

We also certify that the Bidder and "Name of OEM" have agreed to execute agreement in the above respect subject to the Bidder being selected for the Project and Bidder loading support order on "Name of OEM", a copy of same shall be shared with you, with in 1 month of ordering of support by Bidder

**For Partner**

**For OEM**

**Authorized signatory of Bidder**

**Authorized signatory of OEM**

<<BILL OF MATERIAL>>

**7.3 Format 3: Proposed Solution**

1. The Bidder is required to describe the proposed Technical Solution in this section. Following should be captured in the explanation:
  - Clear articulation and description of the design and technical solution and various components (including diagrams and calculations wherever applicable)
  - Extent of compliance to technical requirements specified in the scope of work
  - Technical Design and clear articulation of benefits to Govt. of various components of the solution vis-à-vis other options available.
  - Strength of the Bidder to provide services including examples or case-studies of similar solutions deployed for other clients.
2. The Bidder should provide detailed design and sizing calculation for the following listing all assumptions that have been considered:
  - a. SOC Solution Implementation
  - b. Operations and Maintenance of SOC including manpower
2. Approach & Methodology for O&M of SOC and adherence to SLAs.
3. Bidder shall provide a detailed project plan with timelines, handing over and taking over process, resource allocation, milestones etc. for Implementation and Operations & Maintenance of the SOC.

**7.4 Format 4: Project management Plan**

The Bidder shall give a detailed description of Project Management Plan for O&M activities for SOC. Any Best practices that it would use could also be mentioned. Typical questions that would need to be answered include:

- 7.4.1** What kind of hierarchy for Project Management does the Bidder propose?
- 7.4.2** What issues generally arise with regard to Project management of SOC Projects?
- 7.4.3** How the Bidder plans to mitigate any risks with regard to project management?
- 7.4.4** How Bidder proposes to deploy manpower for Implementation and O&M Operations?
- 7.4.5** Implementation and O&M plan

**7.5 Format 5: Core Project Team**

Bidder shall provide a detailed description of the proposed Core Project Team to be deployed for the Implementation and O&M of SOC. The description should include details about the Project Team hierarchy and a detailed explanation of the role to be played by each individual that would be part of the team.

## Section VIII– Formats to Response to the RFP: Financial Bid

### 8.1 Format 1: Financial Bid Letter

To,

DGM (Technical)  
Gujarat Informatics Limited  
Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Sir/Madam,

Subject: Selection of Agency for Establishment and Management of on premise Security  
Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST,  
Government of Gujarat

**Reference: RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

We, the undersigned Bidder, having read and examined in detail all the Bid documents in respect of Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat do hereby propose to provide services as specified in the Tender documents number **<Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

#### 1. PRICE AND VALIDITY

- All the prices mentioned in our Bid are in accordance with the terms as specified in the Bid documents. All the prices and other terms and conditions of this Bid are valid for a period of 180 calendar days from the date of opening of the financial Bids.
- We hereby confirm that our Bid prices are exclusive all taxes. However, all the applicable taxes are quoted separately under relevant sections.
- We have studied the clause relating to Indian Income Tax and hereby declare that if any Income Tax, surcharge on Income Tax, Professional and any other corporate Tax is altered under the law, we shall pay the same.

#### 2. UNIT RATES

We have indicated in the relevant schedules enclosed the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

#### 3. DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the Bid documents Further we agree that additional conditions, if any, found in the bid documents, shall not be given effect to.

4. TENDERPRICING  
We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in RFP document.
5. QUALIFYING DATA  
We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.
6. BIDPRICE  
We declare that our Bid Price is for the entire scope of the work as specified in the Schedule of Requirements and RFP documents. These prices are indicated in Formats (Section 8.2) of this Section attached with our bid as part of the RFP.
7. CONTRACT PERFORMANCE GUARANTEE BOND  
We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed in Volume I, Annexure 3- Performa and as per Section IV - General Conditions of Contract.
8. We hereby declare that our Bid is made in good faith, without collusion or fraud and the Information contained in the Tender is true and correct to the best of our knowledge and belief.
9. We understand that our Bid is binding on us and that you are not bound to accept a bid you receive.
10. We confirm that no Technical deviations are attached here with this financial offer.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Printed Name Designation

Seal Date:

Business Address:



**8.2 Format 2: Price/Financial Bid**

| Schedule- I  |  |            |                    |                     |
|--------------|--|------------|--------------------|---------------------|
| Component    |  | Total      | Unit Rate Inc. GST | Total Rate Inc. GST |
| Sr. #        | Device Description   | Qty. (UOM) |                    |                     |
| 1.           | SIEM & SOAR Platform   | 1          |                    |                     |
| 2.           | SIEM & SOAR Platform CAMC & Warranty Support 5 Year          | 1          |                    |                     |
| 3.           | Threat Intelligence Feed                                     | 1          |                    |                     |
| 4.           | Threat Intelligence Feed CAMC & Warranty Support 5 Year      | 1          |                    |                     |
| 5.           | Video Wall   | 1          |                    |                     |
| 6.           | Video Wall CAMC & Warranty Support 5 Year                    | 1          |                    |                     |
| 7.           | Workstation with dual monitor                                | 8          |                    |                     |
| 8.           | Workstation with dual monitor CAMC & Warranty Support 5 Year | 8          |                    |                     |
| 9.           | Operations and Maintenance of SOC for 5 year                 | 1          |                    |                     |
| <b>Total</b> |  |            |                    |                     |

**Note:**

1. L1 will be the lowest sum total of rates with taxes.
2. The yearly CAMC & OEM support cost should not be less than 7% of the CAPEX cost as per. In case of any bidder is quoting less than 7%, the bid is liable to be rejected.
3. Sum Total of AMC & Warranty would be paid in 20 equated Quarters from the date of successfully completion of FAT.
4. RA has been enabled in the GEM Bid.

**Annexure 1: RFP Document Acknowledgement Form**

Dated:

To,

DGM (Technical)

Gujarat Informatics Limited

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Dear Sir,

We hereby acknowledge receipt of a complete set of RFP Documents consisting of Annexure (along with their Appendices) enclosed to the "Invitation for Bid" pertaining to providing of \_\_\_\_\_services against RFP no.\_\_\_\_\_.

We have noted that the closing date for receipt of the RFP by GIL is\_\_\_\_\_at < > hrs. and opening at < > hrs. on the same day.

We guarantee that the contents of the above said RFP Documents will be kept confidential within our organization and text of the said documents shall remain the property of GIL and that the said documents are to be used only for the purpose intended by GIL.

Our address for further correspondence on this tender will be as under:

Telexno:.....

Fax no: ..... Telephone no: .....

Personalattentionof:..... (ifrequired)

Yours faithfully,

(Bidder) Note: this form should be returned along with offer duly signed.

**PERFORMANCE BANK GUARANTEE**  
(To be stamped in accordance with Stamp Act)

Ref: Bank Guarantee No.

Date:

To  
**DGM (Tech)**  
**Gujarat Informatics Limited,**  
**Block -2, 2<sup>nd</sup> Floor, Karmyogi Bhavan,**  
**Sector – 10A, Gandhinagar.**  
**(Gujarat)**

Dear Sir,

1. WHEREAS..... (Name of Bidder) hereinafter called "the Bidder" has undertaken, in pursuance of Agreement dated, ..... (hereinafter referred to as "the Agreement for **Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat** AND WHEREAS it has been stipulated in the said Agreement that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.
2. WHEREAS we \_\_\_\_\_ ("the Bank", which expression shall be deemed to include its successors and permitted assigns) have agreed to give the Government of Gujarat ("GoG") the Guarantee: THEREFORE the Bank hereby agrees and affirms as follows:  
The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to GoG under the terms of their Agreement dated \_\_\_\_\_. Provided, however, that the maximum liability of the Bank towards GoG under this Guarantee shall not, under any circumstances, exceed \_\_\_\_\_ in aggregate.
3. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from GoG in that behalf and without delay/demur or set off, pay to GoG any and all sums demanded by GoG under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from GoG to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:  
  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
Attention Mr. \_\_\_\_\_.
4. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of months from the date of its execution. The Bank shall extend the Guarantee for a further period which may mutually decide by the bidder and GoG. The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged, or otherwise affected by:
  - Any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.
  - Any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or future, between Bidder and the Bank.
5. The BANK also agrees that GoG at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the BIDDER and notwithstanding any

security or other guarantee that GoG may have in relation to the Bidder's liabilities.

- 6. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of GoG or any other indulgence shown by GoG or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.
- 7. This Guarantee shall be governed by the laws of India and the courts of Ahmedabad shall have jurisdiction in the adjudication of any dispute which may arise hereunder.

Dated this the ..... Day of .....

Witness

(Signature)

(Signature)

(Name)

(Name)

Bank Rubber Stamp

(Name)

(Official Address)

Designation with Bank Stamp

Plus Attorney as per Power of Attorney No.

Dated:

**Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative and Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. EMD/10/2021/7729/DMO dated 12.04.2021 issued by Finance Department or further instruction issued by Finance department time to time.**

**Format of Earnest Money Deposit in the form of Bank Guarantee**

Ref: \_\_\_\_\_ Bank Guarantee No. \_\_\_\_\_  
Date: \_\_\_\_\_

To,  
DGM (Technical)  
Gujarat Informatics Limited  
Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,  
Sector 10A, Gandhinagar, Gujarat 382010

Whereas ----- (here in after called "the Bidder") has submitted its bid dated ----- in response to the RFP No. <<<<>>> for <<<<>>> by these presents that WE ----- having our registered office at ----- (hereinafter called "the Bank") are bound unto the \_\_\_\_\_, Gujarat Informatics Limited in the sum of ----- for which payment well and truly to be made to Gujarat Informatics Limited , the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this -----day of -----2021.

THE CONDITIONS of this obligation are:

1. The E.M.D. may be forfeited:
  - a. if a Bidder withdraws its bid during the period of bid validity
  - b. Does not accept the correction of errors made in the tender document;
  - c. In case of a successful Bidder, if the Bidder fails:
    - (i) To sign the Contract as mentioned above within the time limit stipulated by purchaser or
    - (ii) To furnish performance bank guarantee as mentioned above or
    - (iii) If the bidder is found to be involved in fraudulent practices.
    - (iv) If the bidder fails to submit the copy of purchase order & acceptance thereof.

We undertake to pay to the GIL/Purchaser up to the above amount upon receipt of its first written demand, without GIL/ Purchaser having to substantiate its demand, provided that in its demand GIL/ Purchaser will specify that the amount claimed by it is due to it owing to the occurrence of any of the abovementioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to the validity of Bids 9 Months. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the OWNER/PURCHASER and further agrees that the guarantee herein contained shall continue to be enforceable till the OWNER/PURCHASER discharges this guarantee

The Bank shall not be released of its obligations under these presents by any exercise by the OWNER/PURCHAER of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the OWNER/PURCHASER or

any other indulgence shown by the OWNER/PURCHASER or by any other matter or things.

The Bank also agree that the OWNER/PUCHASER at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the OWNER/PURCHASER may have in relation to the SELLER's liabilities.

Dated at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 2021.

\_\_\_\_\_

Signed and delivered by

\_\_\_\_\_

For & on Behalf of

Name of the Bank & Branch &  
Its official Address

Approved Bank: Any Nationalized Bank operating in India having branch at Ahmedabad/  
Gandhinagar

**On letterhead of Bidder**

**Sub : Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division**

**Ref: Bid Number:** \_\_\_\_\_

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that we as a bidder and quoted product from following OEMs are not from such a country or, if from such a country, these quoted products OEM has been registered with competent authority. I hereby certify that these quoted product & its OEM fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number \_\_\_\_\_.

| No. | Item Category | Quoted Make & Model |
|-----|---------------|---------------------|
|     |               |                     |
|     |               |                     |
|     |               |                     |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

**On letterhead of OEM**

**Sub : Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020  
published by Ministry of Finance, Dept. of Expenditure, Public Procurement division**

**Ref: Bid Number:** \_\_\_\_\_

Dear Sir,

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that our quoted product and our company are not from such a country, or if from such a country, our quoted product and our company have been registered with competent authority. I hereby certify that these quoted product and our company fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number \_\_\_\_\_.

| No. | Item Category | Quoted Make & Model |
|-----|---------------|---------------------|
|     |               |                     |
|     |               |                     |
|     |               |                     |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority; otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**



**Selection of Agency for Establishment and  
Management of on premise Security Operation  
Center (24x7x365 days) at Gujarat State Data  
Center, Gandhinagar,  
DST, Government of Gujarat.  
Volume-II  
(Scope of Work and SLAs)**



**Gujarat Informatics Ltd  
Block No. 2, 2nd Floor,  
C & D Wing, Karmayogi Bhavan  
Sector - 10 A, Gandhinagar – 382010 Gujarat.**

**Ph No. 23252026, 23258692**

**Fax: 23238925.**

**<https://gil.gujarat.gov.in>**

**Abbreviations**

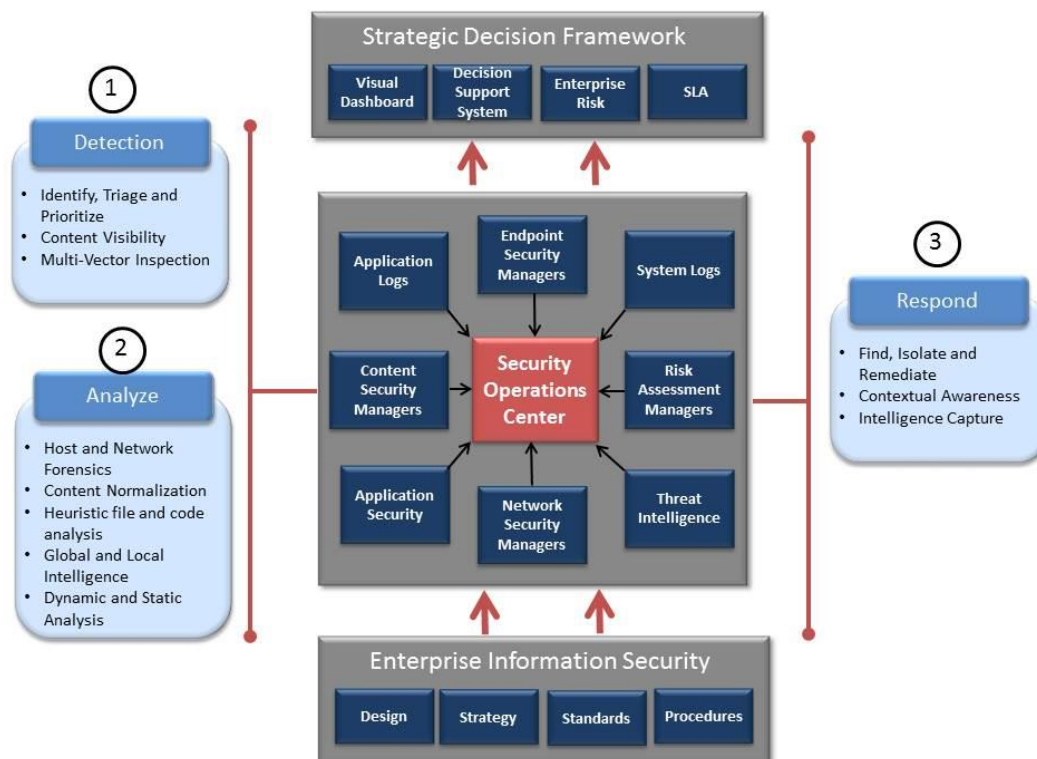
1. **GoG:** Government of Gujarat
2. **DST:** Department of Science & Technology
3. **GIL:** Gujarat Informatics Limited
4. **GSWAN:** Gujarat State Wide Area Network
5. **GSDC:** Gujarat State Data Centre
6. **SOC:** Security Operations Center
7. **OEM:** Original Equipment Manufacturer
8. **O&M:** Operations & Maintenance
9. **EMS:** Enterprise Management Suite
10. **NMS:** Network Monitoring System
11. **EMD:** Earnest Money Deposit
12. **PBG:** Performance Bank Guarantee
13. **SLA:** Service Level Agreement
14. **FAT:** Final Acceptance Test
15. **TPA:** Third Party Agency
16. **SoW:** Scope of Work
17. **SIEM:** Security Information and Event Management
18. **SOAR:** Security Orchestration, Automation and Response
19. **CCTV:** Closed Circuit Tele Vision
20. **QP:** Quarterly Payment
21. **TENDERER:** DST/GIL/ Government of Gujarat

## Section I: Introduction

### 1.1. Security Operations Center (SOC)

Government of Gujarat (GoG) has decided to set up Security Operations Center (SOC) in Gandhinagar, the State capital. SOC will monitor, prevent, assess, detect, respond, and defend Government of Gujarat's critical information systems and IT infrastructure of state against cyber threats.

The countless interconnections among diverse actors, networks, applications, systems, and computing devices create a network of interdependencies in which the health of one component can impact the health of the ecosystem itself. Key to developing an effective SOC is recognizing and understanding environment. An unprotected computer can open doors to a plethora of trusted networks; a successful Denial-of-Service attack can slow networks or interrupt services for the entire IT infrastructure. Left unchecked, malware could sweep like a pandemic through the environment. Although interconnections within the environment can create vulnerabilities, they also enable SOC to conduct effective operations by working collaboratively to gather and analyse information and respond to attacks.



**Detection Stage** - This phase would involve the collection of threat feeds from various devices/equipment/applications spread across the different locations. These feeds would be primarily provided visibility and insight into the entire network traffic being generated across the IT Infrastructure of GoG; these feeds are incorporated into the SoC to provide visibility into the entire architecture. Detection stage leverages the following technologies to identify, Triage and Prioritize response against sophisticated cyber threats. This helps in content visibility and Multi-Vector Inspection.

**Analyze Stage** - During this phase advance analysis is undertaken based on the information collected and discovered in the Detection stage. Activities undertaken in this stage primarily involve detecting anomalies/ behavioural changes in the network infrastructure, threats against various assets in the network and their corresponding vulnerabilities. This Stage would involve deep host and network forensics, content normalization, Heuristic file and code analysis leveraging the following technologies.

**Respond Stage** - Once the attack has been detected after analysis, the appropriate action needs to be undertaken in the most automated manner, which would involve blocking of real time threat and attacks across the network infrastructure of GoG. Response should focus on to identify, isolate, and remediate threats. Response leverages detection and analysis framework to enrich contextual awareness and intelligent capturing. Each of the above defined stage provides input at each level of collection, analysis, confirmation and as far as possible automated responses to the alerts and incidents created across the enterprise-wide dashboard.

## Section II: Scope of Work

Gujarat Informatics Limited on behalf of Department of Science and technology, Government of Gujarat issued this RFP for Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat. DST envisages setting up of SOC at GSDC Gandhinagar for the critical infrastructure of state like GSDC, GSWAN, SICN, GISL etc.

The scope of work under this RFP is Selection of Agency for Establishment and Management of on premise Security Operation Center (24x7x365 days) at Gujarat State Data Center, Gandhinagar, DST, Government of Gujarat.

### 1.1. Establishment and Management of on premise SOC:

- 1.1.1. Bidder is required to supply, install, configure, test and commission the required Hardware, software and compute (inclusive of all active & passive components and subcomponents, accessories) as per the technical and functional specification mentioned in the RFP document.
- 1.1.2. The licenses supplied by the selected bidder should be in the name of Department of Science and Technology, Government of Gujarat valid perpetual for life and handover to SOC.
- 1.1.3. Bidder is required to provide Racks with iPDU & other components
- 1.1.4. Required Power point within each rack will provided by SOC/DST. However, bidder will have to ensure that the hardware supplied/delivered is compatible with the IPDU's supplied in the rack or bidder needs to provide required connector, if any.
- 1.1.5. The bidder should provision the required hardware and software components which mentioned in the RFP to be implemented under this RFP Scope.
- 1.1.6. The Bidder has to ensure that if any additional component(s) required for overall solution to comply with the implementation to achieve desired objectives and SLA levels, then in such case it should be the responsibility of the bidder to provide the same as a part of the entire solution.
- 1.1.7. The architecture needs to be scalable to meet future demand.
- 1.1.8. Bidder shall be responsible for setting up of on premise SOC at GSDC premises and provide the required security services for period of 5 years. The Onsite resources (People, Process and Technology) required to run and manage the SOC shall be deployed from the bidder's own sources to manage, monitor, analyze and report incidents as they occur
- 1.1.9. The requirements in the captive Security Operations Centre (SOC) shall at the minimum include the following functionalities/capabilities. Accordingly, the bidder shall:
  - 1.1.9.1. Implement, Integrate, customize, manage, and maintain Security Information & Event Management (SIEM), SOAR, Threat intelligence feed technologies and Resources to meet SOC/DST's Requirements.
  - 1.1.9.2. Perform gap analysis between the SOC/DST's requirements and the services functionality of SIEM, SOAR product and other tools and technologies
  - 1.1.9.3. Setup and configure Case Management tools and technologies to automate the case management and workflows to mitigate the gaps.
  - 1.1.9.4. Setup SOC solution as a framework that is comprehensive, scalable and addresses all security aspects.
  - 1.1.9.5. Integrate and Monitor security incidents of tools/devices - Network, Security, and other devices
  - 1.1.9.6. Manage and carry out rule-based Audit of Security Devices:
    - Firewalls
    - IPS
    - SOC Rules Intelligences

- SOC Operations
- 1.1.9.7. Build custom interfaces if required for integration
- 1.1.9.8. Provide Security Intelligence for SOC Solutions
- 1.1.9.9. Provide post implementation monitoring & management support.
- 1.1.9.10. Integrate any other device procured by the SOC/DST.
- 1.1.9.11. Provide on-site monitoring services for
  - 24x7x365 Real-time Security Monitoring in a Fully Managed Service Delivery Model
  - Correlation of event logs with other relevant security information including vulnerability information, network flows and external threat intelligence
  - Leverage the SIEM solution detect, analyze, and qualify security alerts for various use-cases
  - Escalate qualified security incidents to SOC/DST for further investigation.
  - Create incident tickets in a ticketing tool for the qualified incidents and alerts
  - Analyze false positives and recommend modification/deletion of correlation rules.
  - Provide remediation recommendations.
  - 24x7x365 SOC Tools & SOC Infrastructure Administration and Support in a Co-Managed Service Delivery Model
  - Perform Health and Availability monitoring and notification of the SOC solution
  - Perform Validation of successful configuration backup and log archival based on SOC/DST policies
- 1.1.9.12. Provide single integrated and consolidated enterprise view of security and compliance in the dashboard
- 1.1.9.13. Provide roll-out plans for each of the deliverable and adhere to the same
- 1.1.10. Bidder has to submit the HLD, LLD, detailed project plan etc. for SOC. It is preferable that configuration, Implementation, and commissioning will be done by respective OEM for particular device.
  - 1.1.10.1. Bidder should provide the overall program management and should undertake OEM support for their respective technologies from various OEMs so as to ensure seamless implementation as per the design goals.
  - 1.1.10.2. The OEM resources should be engaged to collect the Customer requirement to achieve business outcomes and based upon that provide the specific solution designing (OEM High-Level & Low-Level Design) with Implementation & configuration implementation support to the bidder for deployment. OEM should also provide a test plan that should be executed by the bidder before go-live to ensure that OEM supplied technology & products work as per the design objectives.
  - 1.1.10.3. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with SOC to meet their business requirements.
  - 1.1.10.4. The bidder shall obtain sign-offs from OEM on the system design & deployment architecture before go-live of the envisaged system and submit before FAT.
- 1.1.11. The support including spares, patch updates, for the quoted products shall be available for the entire period of the Project without any additional cost.
- 1.1.12. Successful bidder is required to undertake the Operation and Maintenance of the entire solution on completion of FAT.
- 1.1.13. The bidder needs to provide a comprehensive, on-site training on deployed solution to the team nominated by SOC/DST, GoG.
- 1.1.14. **Warranty Support:** As part of the warranty services bidder shall provide:
  - 1.1.14.1. Bidder shall provide a comprehensive on-site and free warranty for 5 years from the date of FAT for proposed solution
  - 1.1.14.2. Warranty and Support of all devices & tools will be considered only after successful FAT date.
  - 1.1.14.3. Bidder shall also obtain the five years OEM premium support (ATS/CAMC) on all licensed software, OSS, any other third-party tool, hardware, and other equipment for providing OEM support during the warranty period.
  - 1.1.14.4. Wherever specific clause is not defined, by default support of all devices and tools should be premium one i.e., 4/6 hrs replacement and according to SLA
  - 1.1.14.5. Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the bid. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this bid against any manufacturing defects during the warranty period.

- 1.1.14.6. Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the bid.
- 1.1.14.7. Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the bid. During the warranty period bidder, shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
- 1.1.14.8. Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipment's for inspection, delivery of equipment's or for commissioning of the systems or for acceptance tests / checks on per site basis, DST/SOC reserves the right to charge a penalty.
- 1.1.14.9. During the warranty period bidder, shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidder notice.
- 1.1.14.10. The bidder shall as far as possible repair/ replace the equipment at site.
- 1.1.14.11. Warranty should not become void, if DST/SOC buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.
- 1.1.14.12. Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
- 1.1.14.13. Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
- 1.1.14.14. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
- 1.1.14.15. To provide warranty support effectively, OEM should have spare depo in India and will be asked to deliver spare as per SLA requirement.
- 1.1.14.16. "After completion of 5 years warranty/CAMC/O&M period, if required, SOC/DST may extend the warranty/CAMC/O&M support for further period of 2 years (6th year and 7th year) on the derived rates of average cost of 5 years warranty/CAMC/O&M cost quoted. Bidder is required to provide the undertaking for the same mentioning that they will provide 6th year and 7th year warranty/CAMC/O&M support".
- 1.1.14.17. The Bidder shall ensure that the products quoted should not be declared "End of Production" for next 5 years and "End of support" for the next 7 years by the OEM from the date of bid submission. However, if OEM declares any equipment/solution/software/or part as end of support for any reasons, then in that case OEM has to replace that equipment with better or equivalent products without any cost to DST/GoG. OEM to provide compliance on their letter head for the specification of Hardware and Software Infrastructure

## 1.2. Key Deliverables:

The bidder needs to provide following deliverables in accordance with the Implementation Timelines.

| S/N | Deliverables                                   | Activity   |
|-----|--|--|
| 1.  | Kick-off meeting                               | <ul style="list-style-type: none"> <li>Project Plan</li> </ul>   |
| 2.  | Delivery of Components                         | <ul style="list-style-type: none"> <li>Software License documents</li> <li>Hardware warranty certificate</li> </ul>  |
| 3.  | Installation & Commissioning                   | <ul style="list-style-type: none"> <li>Solution architecture documents</li> <li>Logical and physical design</li> <li>Completion of UAT and closure of observations</li> <li>Integration Testing Report</li> <li>Test cases &amp; SOPs for the SOC</li> </ul> |
| 4.  | FAT  | <ul style="list-style-type: none"> <li>Successful implementation of SOC solution specifications and functional requirements as mentioned in this RFP</li> </ul>  |
| 5.  | Deployment of manpower proposed for O&M of SOC | <ul style="list-style-type: none"> <li>Required Manpower as per scope of RFP</li> </ul>  |

**1.3. Bill Of Material**

The tenderer is intended to procure following system included but not limited to required Hardware, Software, License, Accessories and any other device / software to full fill the functional requirement mentioned under this RFP.

| Sr. # | Device Description   | Qty. | (UOM) |
|-------|--|------|-------|
| 1.    | SIEM & SOAR Platform   | 1    | Set   |
| 2.    | SIEM & SOAR Platform CAMC & Warranty Support 5 Year          | 1    | Set   |
| 3.    | Threat Intelligence Feed                                     | 1    | Set   |
| 4.    | Threat Intelligence Feed CAMC & Warranty Support 5 Year      | 1    | Set   |
| 5.    | Video Wall   | 1    | Set   |
| 6.    | Video Wall CAMC & Warranty Support 5 Year                    | 1    | Set   |
| 7.    | Workstation with dual monitor                                | 8    | Set   |
| 8.    | Workstation with dual monitor CAMC & Warranty Support 5 Year | 8    | No.   |

**Section III: Technical Specification**

The bidder should provide state of the art solution to fulfil over all functional requirement for SOC. Services to be offered to SOC/DST:

**1. Monitoring and Log Analysis Services**

- 1.1 The devices included in the scope of monitoring & log analysis to be carried out from the SOC to be set up in the SOC/DST's Premises and managed by the Bidder's personnel are as follows:
  - 1.1.1 Monitoring of 1500 devices– Provision to increase 20% every year on SOC/DSTs expansion.
  - 1.1.2 Monitoring & Recording of all ingress points traffic for the above mentioned traffic with full packet capture replay capabilities.
  - 1.1.3 Management of Security devices deployed as per the scope of setting up the Security Operations Center including rule base audit and management of devices creation of rules during non-business hours. Monitoring of 24x7 logs & audit trails for the security events to detect known as well as unknown attacks and raising alerts on any suspicious events that may lead to security breach into SOC/DST's environment. Monitoring of 24x7 performance and service availability so that the desired state and integrity of the devices and services levels are maintained.
  - 1.1.4 To be able to support and provide scalability for any additions/modifications or integration of applications, services, devices and networks with the existing architecture.
  - 1.1.5 Performing Analysis of any suspicious traffic and initiating response in co-ordination with the SOC/DST's IT team
  - 1.1.6 Providing initial review (Level 1) of security incidents and the determination if escalation to Level 2, 3 supports is warranted.
  - 1.1.7 Carrying out event analysis with the statistical events correlation rules. This should include the correlation of the events from the devices under scope.
  - 1.1.8 Creation and adding custom correlation rules for the SOC/DST's devices under scope. SOC will review and fine-tune rules as and when required.
  - 1.1.9 Providing online secured portal (web-based Dashboard) for viewing real-time monitoring data of all the security devices in scope.
  - 1.1.10 To Review, Develop& recommend improvement plans for the SOC monitored SOC/DST's facilities as needed to maintain an effective and secure computing environment. The activity to be carried out once in 6 months.
  - 1.1.11 Monitoring alerts and events reported by devices under the SOC scope; to record the incidents, classify, and recommend remedial action. All types of incidents will have to be reported immediately as per the escalation matrix.
  - 1.1.12 Initiation of prompt corrective countermeasures to stop/prevent attacks as per predetermined procedures.
  - 1.1.13 Complete analysis and correlation of logs from all the devices under scope.
  - 1.1.14 Carrying out due forensic activities to identify the origin of threat, mitigation steps and measures to prevent recurrence.
  - 1.1.15 Preparation of the daily/ weekly / monthly reports to summarize the list of incidents, security advisories, vulnerability management, and other security recommendations. It should include the operations trend analysis with the reports correlation of the present month's operations data with the previous months' data.

**2. Other Security Services:**

- 2.1 Security Threat Intelligence Feed Services
- 2.2 The Bidder shall regularly track and advise the SOC/DST about new global security threats and vulnerabilities. The advisories shall be customized to suit the SOC/DST's/GoG security infrastructure. The Bidder shall advise upgrades / changes in the security infrastructure of the SOC/DST/GoG against evolving threats and responsibilities. Onsite team shall track impact of new vulnerabilities and threats on SOC/DST's/GoG assets. The Bidder should advise and coordinate implementation of controls to mitigate new threats
- 2.3 The Bidder or their onsite team shall ensure adequacy, appropriateness and concurrency of various policies and guidelines in place and shall provide Information Security consultancy for newer technology deployment for new and existing applications and products. Onsite Team shall track and support implementation and coordinate for closure of vulnerabilities on assets that are affected. The Bidder shall provide a security dashboard for online view of the global vulnerabilities and threats applicable to the SOC/DST's/GoG environment, number of assets affected and status of mitigation

**3. Dashboard View:**

- 3.1 The bidder shall provide a SOC a **single dashboard view** of all the integrated devices, tools, applications, and databases for ease of monitoring
- 3.2 The Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department.
- 3.3 The Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats Dashboard should accept CSV, XML, Excel formats to upload data in the dashboard SLA data should be captured in the dashboard with compliance details

**4. SOC Operations Team Specification**

- 4.1 The asset list and service deliverables are provided in this RFP for the bidder to assess the volume of work and accordingly provide adequate personnel with appropriate skills. The minimum team structure is provided in the table below. The table lists the roles, skill sets of personnel required for the above deliverables. The Bidder may respond with additional resources apart from the minimum required based on its assessment of the scope of work, deliverables and SLA

| Sr No | Role  | Qualifications and Experience  | Minimum No of resources | Level |
|-------|---|--|-------------------------|-------|
| 1     | Sr. Security Analyst/ Sr. Technology Specialist | <p>Education: B.E. / B. Tech / MCA degree. Certified with: EC Council-CEH/Comptia Security+/CISSP/CHFI, Proposed OEM certification.</p> <ul style="list-style-type: none"> <li>· 5+ years of relevant experience in managing all aspects of risk and incident analysis in SOC. Must have experience in managing at least 1 projects for enterprise scale Clients.</li> <li>· Shall be responsible for deployment, maintaining, tuning, monitor and managing all aspects of client SOC. Responsible for coordinating, in a timely manner, all activities necessary for security incident monitoring, analysing incidents / risks, incident / risk containment, identifying root cause, initiate problem resolution, incident / risk response and communication.</li> <li>· Shall have experience of monitoring the database security logs/alerts and shall take complete ownership for the same.</li> <li>· Well versed with aspects of database security, access control, identity management, encryption of database, data obfuscation techniques. Should have experience of firewall, IPS, Anti-APT solution etc.</li> </ul> | 3(L2) + 1(L1)           | L2/L3 |
| 2     | Security Analyst                                | <p>B.E/B. Tech/ MCA degree</p> <ul style="list-style-type: none"> <li>· Certified with: OEM Certification/ Certified SOC Analyst (CSA)-</li> </ul>   | 4                       | L1    |



|  |  |  |  |  |
|--|--|--|--|--|
|  |  | EC Council/ CompTIA CySA+  |  |  |
|  |  | · 3+ years of overall experience with at least 1 years of relevant experience in all aspects of Incident monitoring in SOC |  |  |

4.2 General Guidelines:

- 4.2.1 The SOC team will work in 24x7x365 environment and personnel resources should be able to work in shifts and flexible working hours to support the operations.
- 4.2.2 SOC/DST reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.
- 4.2.3 At a later stage also if any of the personnel resources are found unsuitable to perform duties or any of the personnel resources violates any of the SOC/DST guidelines, SOC/DST may seek removal of all such personnel resources.
- 4.2.4 SOC/DST expects to build a strong team and there should be no single point of dependency on any one individual. SOC/DST's services should always remain immune to any such dependencies.
- 4.2.5 Bidder is required to obtain permission from SOC/DST in writing before removing any of the personnel resources from the project.
- 4.2.6 SOC/DST expects deployed resource / personnel resources to constantly keep upgrading their product / domain knowledge & skills.
- 4.2.7 As soon as SOC/DST adopts a newer version of an existing technology, SOC/DST expects the existing staff working in the project to get certified on the same or the Bidder should arrange for the additional resources with requisite qualifications/certifications.
- 4.2.8 Proper on-boarding and off-boarding processes are required to be followed.
- 4.2.9 All the staff are required to abide by the SOC/DST's applicable policies and NDA.
- 4.2.10 The teams should be adequate to ensure the unhindered 24x7x365 operations and support.
- 4.2.11 L3 Engineer /Team Lead would be the single point of contact for SOC/DST.
- 4.2.12 SOC/DST should be provided with a dedicated and exclusive team.
- 4.2.13 A detailed shift roster must be published at the start of the month in consultation with SOC/DST
- 4.2.14 The bidder should factor in an increase of 15% on personnel resources on YoY basis at the agreed cost and Terms & Conditions in this RFP. However, SOC/DST will take a final call on this at its own discretion.
- 4.2.15 The onsite resources must work as per SOC/DST's working days and hours or as decided by SOC/DST for smooth functioning of SOC/DST SOC.
- 4.2.16 Bidder will be responsible for police verification & background checks of all resources before on boarding

Minimum Roles and Responsibilities:

| Resource Level       | Roles & Responsibilities   |
|----------------------|--|
| L1(Security Analyst) | <p>Level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available SOC log sources that include:</p> <ul style="list-style-type: none"> <li>• Firewalls and network devices.</li> <li>• Infrastructure server and end-user systems.</li> <li>• Threat intelligence platforms.</li> <li>• Web proxies.</li> <li>• Application logs and web-application firewalls.</li> <li>• Identity and access management systems.</li> <li>• Cloud and hybrid-IT provisioning, access, and infrastructure systems.</li> <li>• Antivirus systems.</li> <li>• Intrusion detection and prevention systems.</li> </ul> <p>Monitor incoming event queues for potential security incidents.<br/>                     Perform initial investigation and triage of potential incidents and escalate or close events as applicable.<br/>                     Monitor SOC ticket (or email) queue for potential event reporting from outside entities and</p> |

|                          |   |
|--------------------------|---|
|                          | <p>individual users.<br/> Maintain SOC shift logs with relevant activity from the shift.<br/> Document investigation results, ensuring relevant details are reported to level 2 analyst for final event analysis.<br/> Update or refer SOC collaboration tool as necessary for changes to SOC process and procedure as well as ingest SOC daily intelligence reports and previous shift logs.<br/> Conduct security research and intelligence gathering on emerging threats and exploits.<br/> Perform additional auxiliary responsibilities as outlined in the console monitoring procedure.<br/> Communicating emergency alerts &amp; warnings to designated stakeholder/ departments/ SOC.</p>   |
| L2(Sr. Security Analyst) | <p>Monitor SOC Solution Console &amp; Dashboards and provide response to the reported incidents Filtered by L1.<br/> Monitor and review the L1 activities<br/> Support the day-to-day operation of a highly available distributed multi-clustered multi-tenant SOC Solution deployment.<br/> Perform initial analysis for known issues and provide the appropriate recommendations for closure.<br/> Monitor &amp; Reporting of system components health and take necessary action in case of any observed issue.<br/> Provide notification and communication with Incident management and respective application team upon threat detection.<br/> Perform analysis on the reported incidents, determine the root cause, recommend the appropriate solution.<br/> Should provide real time situational awareness to the SOC/DST's stakeholders.<br/> Use and apply learnings from incident and provide recommendation for standardizing the SOC Solution.<br/> Develop and implement processes for interfacing with operational teams and other supporting teams.<br/> Ensure the SOC Solution integration is intact among the SOC/DST SOC solutions, other assets Design, create and customize the dashboards as per the SOC/DST's requirements.<br/> ensure the necessary SOC/DST SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas.<br/> Automating Day to Day Tasks related with SOC Solution Operations (but not limited to)<br/> Above is illustrative list of general activities. All Technology specific activities Related to SOC Solution to be carried out.<br/> SOC Solution Management, SOC Solution Monitoring, SOC Solution Operations, SOC Solution Automation, Content Development to fine-tune existing rules &amp; develop new content based on latest threat vectors. Ensure &amp; keep improving SOC Solution platform for better Return on Investment.<br/> Should have good understanding on MITRE att&amp;ck framework.</p> |

|                               |  |
|-------------------------------|--|
| L3(Sr. Technology Specialist) | <p>Monitor and review the L2 activities<br/>Should provide real time situational awareness to the SOC/DST's stakeholders.<br/>Use and apply learnings from incident and provide recommendation for standardizing the SOC Solution.</p> <p>Ensure the SOC Solution integration is intact among the SOC/DST SOC solutions, other assets<br/>Design, create and customize the dashboards as per the SOC/DST's requirements.<br/>Ensure the necessary SOC/DST SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas.</p> <p>Support on boarding and maintenance of a wide variety of data sources to include various OS, appliance, and application logs.</p> <p>Create Custom queries, custom dashboards, and visualizations to support SOC/DST's requirements and monitoring of the SOC Solution deployment</p> <p>Create and manage SOC Solution knowledge objects to include apps, dashboards, saved and scheduled searches and alerts</p> <p>Support access requests and modifications and permissions</p> <p>Support troubleshooting and remediation of issues as they arise with data ingestion and SOC Solution infrastructure</p> <p>Work on Improvement of overall posture of SOC Solution deployment to achieve best return on investment.</p> <p>Review SOC architecture and suggest any updates</p> <p>Monitor &amp; report on cyber threats and suggest any changes needed to protect the organization in SOC Solution, Leading End-to-End Implementation of the suggested changes along with L2. SOC Solution Management, SOC Solution Monitoring, SOC Solution Operations, SOC Solution Automation, Content Development to fine-tune existing rules &amp; develop new content based on latest threat vectors. Ensure &amp; keep improving SOC Solution platform for better Return on investment.</p> <p>Should have a very good understanding on MITRE att&amp;ck framework.</p> |
|-------------------------------|--|

## 5. SOC Tools, Equipments, Platform

5.1 Mentioned below are the requirements of the SOC that the vendor should comply with. Please explain the compliance in the remarks column and with reference to relevant sections in the proposal–

5.2 Following SOC tools must be configured for 99.9% Availability calculated on Quarterly places.

- SIEM Solution and Security Analytics Platform
- SOAR Solution
- Threat Intelligence Feed

### 5.3 SIEM and SOAR

| S. No | Technical Requirements  | Compliance (Y/N) |
|-------|---|------------------|
| 1     | Proposed solution must be platform supporting Visibility, detection, investigation, and response  |                  |
| 2     | Next Gen Platform must enable SDC to: <ul style="list-style-type: none"> <li>- Gain complete visibility into security data from a single pane</li> <li>- Reduce events into a prioritized list of the most important alerts</li> <li>- Leverage automated, advanced analytics and threat intelligence to speed investigation time</li> <li>- Scale rapidly with out of the box use cases and integrations</li> <li>- Drive compliance and manage regulatory risk</li> </ul> |                  |
| 3     | Must Support a wide variety of technologies, applications, and cloud services to help customers gain comprehensive visibility into enterprise-wide activity   |                  |
| 4     | The solution Should include pre-built Device Support Modules, Solution must be capable of simple ingesting data from number and variety of log sources  |                  |

|    |  |  |
|----|--|--|
| 5  | <p>Solution Must intelligently correlates and analyses a variety of data types from a wide range of sources, including the following:</p> <ul style="list-style-type: none"> <li>– Endpoint data: from the Windows event log, Sysmon, nmon , EDR solutions and more</li> <li>– Network activity data: from firewalls, gateways, routers, switches or sensors</li> <li>– Vulnerability data: From antivirus tools, vulnerability scanners, intrusion detection systems, intrusion prevention systems, data loss prevention systems and more</li> <li>– Cloud activity: From SaaS and IaaS environments, such as Office365, Salesforce.com, Amazon Web Services (AWS), Microsoft Azure and Google Cloud</li> <li>– User and identity data: Ingested from Active Directory, LDAP, or other identity and access management solutions</li> <li>– Application data: From enterprise resource planning (ERP) &amp; COTS solutions, application databases, SaaS applications, Mail solution and more</li> <li>– Threat intelligence: From third-party &amp; Open Source threat intelligence feeds</li> <li>– Container activity data: from container management</li> </ul> |  |
| 6  | Next gen Platform must include Data Lake, Security Analytics, Log Forensics, Ingestion from variety of sources including Applications, OT, IT, Network and Security  |  |
| 7  | SIEM solution must apply intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions   |  |
| 8  | The proposed solution should be sized for sustained data of 25,000 EPS or equivalent Gb/day or equivalent CPU - capacity based at all layers but should be able to handle peak of 50,000 EPS or equivalent GB/day or equivalent CPU - capacity based at all layers without dropping events or queuing events and must take burst of 100000 EPS or equivalent GB/Day. There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till the time data ingestion size remains as per ask  |  |
| 9  | Proposed solution must be enterprise highly scalable solution with Analytics and predictive capabilities.  |  |
| 10 | Data Ingestion should be fast and OEM solution must be capable of ingesting data from all IP sources also including Applications both home grown and commercial off the Shelf applications. In case of parsing requirement for any customised device or applications, it must be owned by OEM to provide same in 7 days, so that organization should not get non-compliant or should have any threats unidentified.  |  |
| 11 | In case of any version change or version upgrade of devices, OEM must ensure data ingestion should not stop and there should not be any data loss  |  |
| 12 | The Proposed solution should have capability to collect logs from most of the standard platforms like Microsoft Windows, Linux (All flavours), MAC OS,AIX, Solaris, Firewalls, Network, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers, Web servers, private cloud etc.   |  |
| 13 | The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks   |  |
| 14 | The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc (High availability)   |  |
| 15 | The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.   |  |
| 16 | The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.   |  |
| 17 | The proposed solution must provide for secure user access via HTTPS, ssh.  |  |
| 18 | The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.  |  |
| 19 | The Proposed solution must offer all the below built-in threat detection techniques out  |  |

|    |   |  |
|----|---|--|
|    | <p>of the box:</p> <ol style="list-style-type: none"> <li>1. Detect Web Application Threats.</li> <li>2. Detect APT Threats.</li> <li>3. Integrate with leading HoneyPot solutions.</li> <li>4. Integrate with leading NBAD, NDR tools.</li> <li>5. Give visibility of endpoints also by integrating with EDR, DLP, HIPS, Antivirus etc for endpoint analytics.</li> <li>6. Integrate with SOAR tools for automation.</li> <li>7. Integrate with leading Threat intelligence Platform (TIP).</li> </ol> |  |
| 20 | The proposed solution must provide a query interface that allows users to search for data stored within the solution.   |  |
| 21 | The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.   |  |
| 22 | The solution should be able to part and filter logs based on type of logs, date etc.  |  |
| 23 | The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data.   |  |
| 24 | The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure   |  |
| 25 | Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business  |  |
| 26 | <p>The proposed solution must be able to read data input from the following static log file formats:</p> <ol style="list-style-type: none"> <li>a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)</li> <li>b. Windows Events Logs</li> <li>c. Standard Log Files from applications such as Web (HTTP/HTTPS) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.</li> </ol>                                 |  |
| 27 | The solution must be able to provide the capability to fully customise alerts, reports, and dashboards to the business requirements.  |  |
| 28 | The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc to provides rapid insights and operational visibility into large-scale Unix and Linux environments machine data: syslog, metrics, and configuration files.   |  |
| 29 | Solution must be capable of providing real time and on demand access to data sources such as evolving format, Custom API's, interfaced incl. text, XML, JSON, Data Base connections, Network Ports, Connections, and files  |  |
| 30 | The solution must be able to provide the capability to annotate events, modify status, build a chronological timeline for the incident before and after a triggered event.  |  |
| 31 | The solution must be able to assign any arbitrary risk score to any data point or fields, example: username, host name, location etc.   |  |
| 32 | The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.   |  |
| 33 | The solution must be able to support multiple transport mechanisms such as TCP, STIX and Trusted Automated exchange of Indicator Information (TAXII).   |  |
| 34 | The proposed solution must be able to provide parsing of custom data sources  |  |
| 35 | The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or reindexing so that complex report or user defined reports can be built.  |  |
| 36 | <p>The solution must be able to support the following indicators:</p> <ul style="list-style-type: none"> <li>- Network, IP</li> <li>- HTTP Referrer, User Agent, Cookie, Header, Data, URL</li> <li>- Domain</li> <li>- Endpoint</li> </ul>   |  |

|    |  |  |
|----|--|--|
|    | <ul style="list-style-type: none"> <li>- File Hash, Name, Extension, Path and Size</li> <li>- Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data</li> <li>- Process Name, Arguments, Handle Name, Handle Type</li> <li>- Service Name, Description</li> <li>- Certificate</li> <li>- Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm</li> <li>- Email</li> <li>- Email Address, Subject Body</li> </ul>  |  |
| 37 | <p>Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, AV, EDR, Firewall (all with Well Known OEM's as well as Open source platforms).</p> <p>Solution should support machine driven triaging algorithms that considers contextual parameters, historical behaviour, and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same</p> <ul style="list-style-type: none"> <li>· Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert.</li> <li>· Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on.</li> <li>· Central Threat Intelligence feed should also be applied to identify threats through known bad actors</li> </ul> |  |
| 38 | <p>Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters</p>  |  |
| 39 | <p>Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise (IOCs), external network connections.</p>  |  |
| 40 | <p>The proposed solution must support real-time remote indexing of data sources to minimize the opportunity for alteration of audit trails on compromised hosts.</p>   |  |
| 41 | <p>Solution should support models to build up the entire attack chain from attack inception, progress of the attack and spread to attack in the network.</p>   |  |
| 42 | <p>The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for correlation and machine learning models.</p>   |  |
| 43 | <p>Solution should support features to identify attacker attributes including threat intelligence score of attackers, who-is lookup information, geomapping in a single console.</p>   |  |
| 44 | <p>Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioural based use cases.</p> <ul style="list-style-type: none"> <li>-Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time</li> <li>-Using distance formula to detect geographically improbable access</li> <li>-To measure the randomness of domain names that can be potentially from malware domain generated algorithms.</li> </ul>  |  |
| 45 | <p>Solution should support integration with open source or commercial IOC sources. List the supported sources which can be integrated with Solution and brief on the integration approach. Solution should support features to analyse and identify the impact of this attack on other assets.</p>   |  |
| 46 | <p>Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.</p>  |  |
| 47 | <p>The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide</p>   |  |

|    |  |  |
|----|--|--|
|    | analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.   |  |
| 48 | The proposed solution machine learning capabilities must include API access, role-based access controls for machine learning models.   |  |
| 49 | The proposed solutions machine learning capabilities must allow addition of custom machine learning algorithms from popular open-source Python libraries.  |  |
| 50 | The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure   |  |
| 51 | Solution should capability to filter undesired, non-security logs at collection, processing, and visualization layer   |  |
| 52 | The proposed solution must be able to read data input from the following static log file formats:<br>a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)<br>b. The solution must be able to accept the following live data streams from cloud server less functions like raw or JSON formatted data over HTTP/HTTPS. |  |
| 53 | The proposed solution should be able to consume logs from any log source without writing parser beforehand or while integration. Parsers should be built once log is ingested  |  |
| 54 | Solution should provide capability to search raw and indexed logs as full text, natural language, time range values, IPs, IP subnet mathematical & statistical functions, logical operators, occurrences count, regex, similar events, first & last seen, predictive & prescriptive search suggestions etc.  |  |
| 55 | Solution should be capable of retrieving the archived logs for reporting, analysis, correlation, investigation, and forensics.   |  |
| 56 | The report should be parameterized, and the user should be able to scale the parameter as needed and Out-of-box aging analysis of incident should be available. Solution should support dynamic reports scheduling and prioritization.   |  |
| 57 | The solution should provide detection/correlation of logs with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open-Source TI feeds)  |  |
| 58 | The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules  |  |
| 59 | The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioural based, etc., across different devices and applications   |  |
| 60 | The solution should have the ability to correlate all the field present in a log/flow data.  |  |
| 61 | The solution should provide a web-based, user-friendly console or a wizard-based console to create rule.   |  |
| 62 | The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix, and Linux environments machine data: syslog, metrics, and configuration files.   |  |
| 63 | The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open-source libraries like NLP, Python etc  |  |
| 64 | The proposed solution should have the ability to perform free text search on events, incidents, rules, and other parameter   |  |
| 65 | The platform should provide the capability to use Machine Learning models on the data  |  |
| 66 | The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.                |  |
| 67 | Machine learning should be embedded across the platform (SIEM, SDL). It should empower every user in the SOC with ML. Solution should use predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate           |  |

|    |  |  |
|----|--|--|
|    | advanced ML frameworks.  |  |
| 68 | The solution should also be capable of collecting and indexing machine data from all the log sources including OS platforms, Middleware, Databases, network & security devices, applications etc., and allow for collecting, indexing, searching, monitoring, and analysing logs in real-time  |  |
| 69 | The solution should have an inbuilt parsing mechanism to be able to parse the logs obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications etc. and convert them into a standard log format on which the analysis can be done. Custom parsing shall also be available for custom applications, if out of the box parsing is not available.  |  |
| 70 | The solution should have the capability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field  |  |
| 71 | The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing url parameters to any third-party website. The Report should be scalable IP-wise, device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.   |  |
| 72 | The solution should have pre-defined rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications etc. as well as threat feeds obtained from different sources   |  |
| 73 | The proposed solution should have ML capabilities.   |  |
| 74 | The solution should offer the flexibility to develop customized correlation rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources on multiple parameters (like Hosts, Geographies, recurring activities) including OS platforms, network & security devices, applications etc. as well as threat feeds obtained from different sources  |  |
| 75 | The solution should have capability of conducting detailed analytics, business intelligence analytics, machine learning, pattern analysis, trends & spikes, anomaly detection, etc   |  |
| 76 | The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc)  |  |
| 77 | The solution should have capability of conducting search across real-time and historical data as and when required   |  |
| 78 | The proposed solution must provide the following capabilities as a Security Analytics Platform:<br>a. One single syntax that can be used universally for search queries, alerts, reports, or dashboards, SIEM, SBDL.<br>b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure<br>c. Risk management technique to apply risk scores to any asset or user based on relative importance or value to the business.<br>d. Threat intelligence technique that automatically collect, aggregate, deduplicate indicators of compromise from threat feeds |  |
| 79 | The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre-defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, R, Python etc.   |  |
| 80 | The solution should have monitoring and alerting capabilities for individual and correlated real-time events   |  |
| 81 | The solution must detect and alert on following:<br>- Firewall port scans<br>- Brute force attack<br>- Network intrusions or suspect traffic   |  |



|    |   |  |
|----|---|--|
|    | <ul style="list-style-type: none"> <li>- Backdoors and Trojans connections</li> <li>- Connect to/from bad/blocked URLs - Analyse web proxy data for connections to malicious URLs</li> <li>- Emerging Threats</li> <li>- Detect and update on emerging threats</li> <li>- Notify security incidents via Voice/Portal/Email</li> <li>- Daily/Monthly report on security monitoring service</li> <li>- Alert in case unavailability of event logs from registered device</li> <li>- TOR, DNS tunnelling kind of malicious communications</li> <li>- DNS query for malicious domains.</li> <li>- Detect suspicious object that are embedded within files through malicious PowerShell scripts for opening a command shell</li> </ul> |  |
| 82 | Solution must provide capability of Log Filtering all logs are not needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.   |  |
| 83 | The solution should provide a pluggable framework to make use of APIs. The framework should support ingestion of data from other applications, export of data from the solution using APIs as well as orchestration of triggers. This solution should provide the ability to use this capability to integrate with other applications for automating tasks and workflows.   |  |
| 84 | The proposed solution should provide end-to end capability to setup an Analytics Platform for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured / semi structured data generated within the organization.   |  |
| 85 | The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics, and performance data for specific formats so that the analyst can have end to end visibility of the ecosystem.   |  |
| 86 | The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies, and outliers across all the data etc. from a single dashboard.  |  |
| 87 | The proposed solution must possess built-in feature for anomaly detection: <ul style="list-style-type: none"> <li>a. Uses historical data as a baseline to forecast future patterns, thresholds, and tolerances</li> <li>b. Ability to identify the future needs of critical system resources, in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results</li> </ul>  |  |
| 88 | Dynamic, intuitive, parameterized, and customizable dashboards should empower personnel resources in the SOC to take prudent decisions. Multidimensional, analytical, trend & pattern-based dashboards should be recommended by individual technology based on their own self-learning capability.  |  |
| 89 | Solution should have end to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.  |  |
| 90 | Solution should have capability to ingest, transform, aggregate, and analyse structured, semi structured and unstructured data for security monitoring.   |  |
| 91 | Solution should have ability to provide continuous feedback by self-learning from incidents remediation, profiling, statistical analysis and auto-retrain itself to reduce false positives.   |  |
| 92 | Solution should be capable to monitor and notify whenever any asset integrated with it stops sending logs/ events / flows/ data / traffic /TI etc.,   |  |
| 93 | Solution should be able to provide raw and normalized logs/data storage as per the retention requirements for SIEM technology as outlined in the scope of work in this RFP  |  |

|     |  |  |
|-----|--|--|
| 94  | Solution should be capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real-time security alerts  |  |
| 95  | The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition it should provide a summary of how the attack or detection technique maps to the following:<br>--ATT&CK MITRE, an adversary behaviour model that describes the actions an adversary might take.<br>--Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.<br>--CIS Critical Security Controls<br>--Data types that are referenced within the rules/search and that need to be populate<br><br>--There should be template to upload advisories in an automated manner.<br>--There should be templates to design and trigger work flows automatically.<br>--Any other customizable templates as per department requirements. |  |
| 96  | Solution should support multi-tenancy feature with segregation of data and display for different entities.   |  |
| 97  | Raw, normalized correlated logs shall be stored to the attached storage/SAN/NAS for the future reference and forensic activities in the event of incident.   |  |
| 98  | Solution must be able to store log data both locally and with SAN/NAS integration.   |  |
| 99  | The solution must store logs online for 90 days followed by near Offline storage for 3 years.  |  |
| 100 | Solution must be IPV6 ready.   |  |
| 101 | Solution shall provide real time threat intelligence from at least one commercial and one open-source feed   |  |
| 102 | Threat Intelligence Feed shall be included with the SIEM & SOAR solution for Five (5) year warranty along CAMC period.   |  |
| 103 | Solution must retrofit with any legacy application/ devices/ equipment event sources, which may or may not be able to push logs. It shall be capable of collecting events from all Applications/ devices/ equipment event sources.   |  |
| 104 | Solution must be horizontally and vertically scalable to support increase in EPS/data  |  |

#### 5.4 Threat Intelligence Feed

| S/N      | Threat Intelligence Requirements  | Compliance (Y/N/) |
|----------|---|-------------------|
| <b>1</b> | <b>Scope</b>  |                   |
| 1.1      | The proposed Vendor solution shall provide cyber threat intelligence and attribution information in the area cyber-crime, cyber-espionage, hacktivism, and enterprise security  |                   |
| 1.2      | The proposed Vendor solution shall provide strategic, operational / tactical, and technical threat intelligence.  |                   |
| 1.3      | The proposed Vendor solution shall provide cyber threat intelligence that is relevant to the below SOC/DST entities based on their business sectors and geographical locations:<br>- GSDC<br>-GSWAN<br>-SICN<br>-GISL |                   |

|      |  |  |
|------|--|--|
| 1.4  | The proposed Vendor solution shall identify and track cyber threat actors that are relevant to SOC/DST. The proposed Vendor solution shall provide a summary of the cyber threat actors as part of the submission  |  |
| 1.5  | The proposed Vendor solution shall identify and track the tactics, techniques and procedures (“TTPs”) used by cyber threat actors that is relevant to SOC/DST. The proposed Vendor solution shall provide a brief summary of the TTPs as part of the submission                      |  |
| 1.6  | The proposed Vendor solution shall identify and track attack campaigns by the cyber threat actors that is relevant to SOC/DST. The proposed Vendor solution shall provide a brief summary for the campaigns, as part of the submission   |  |
| 1.7  | The proposed Vendor solution shall maintain a mapping of the cyber threat actors (alias) to those actors tracked by other reputable proposed Vendor solutions. The proposed Vendor solution shall provide the mapping of the cyber threat actors as part of the proposal submission. |  |
| 1.8  | The proposed Vendor solution must have capabilities to generate a risk score or other quantitative risk assessments of the feeds at least in 2 categories - Reliability & Credibility  |  |
| 1.9  | The proposed Vendor solution must support monitoring of Dark Web forums for information related to SOC/DST and provide searching of live raw feeds from these Forums.  |  |
| 1.10 | The proposed Vendor solution must support proactive monitoring of Threat Actor infrastructures such as C&C servers, Telegram/IRC channels, forums, OSINT, Card shops etc.  |  |
| 1.11 | The proposed Vendor solution must provide compromised information related to SOC/DST such as credentials, latest exposed credit cards (masked & unmasked both), Mule Accounts, Files, Mobile Devices etc by proactively monitoring Threat Actor infrastructures.                     |  |
| 1.12 | The proposed Vendor solution must support monitoring of OSINT such as - Pastebin, Ideaone, Github, Virustotal, Anyrun etc for information related to SOC/DST   |  |
| 1.13 | The proposed Vendor solution must provide list of all release vulnerabilities from different vendors both CVE and Non-CVE along with list of known exploits in the wild for the relevant vulnerabilities.  |  |
| 1.14 | The proposed Vendor solution must provide suspicious and malicious list of IPs in the categories of CnC server, DDoS, TOR nodes, BoT and Open Proxies etc  |  |
| 1.15 | The proposed Vendor solution must provide access to a central database of publicly leaked email credentials for easy search & alert if any of the SOC/DST accounts are leaked in public dumps.   |  |
| 1.16 | The proposed Vendor solution must have capability to detect defacement   |  |
| 1.17 | The proposed Vendor solution must provide detection of Phishing attempts, Domains, Phishing pages hidden inside and defacements by proactively monitoring Threat Actor infrastructures.  |  |
| 1.18 | The proposed Vendor solution should provide Cloud based sandbox for SOC/DST to submit files for detonation and inspection of unknown as well-known malware behaviour   |  |

|          |   |  |
|----------|---|--|
| 1.19     | The proposed Vendor solution must provide Network Analytic Graph for Threat Hunting and attribution purposes for SOC/DST Threat Analysts. This linkage graph should act as a single lookup functionality for multiple types of IOCs   |  |
| 1.20     | The proposed Vendor solution must provide detailed analysis of latest Threats by Cyber Criminal and Nation state Groups including but not limited to IOCs, MITREATT&CK mapping, tools used etc. These threat analysis reports should also include but not limited -<br><ul style="list-style-type: none"> <li>- Malware</li> <li>- Campaign</li> <li>- Threat Actor profiles</li> <li>- TTP's</li> <li>- IOCs per threat</li> <li>- Monitoring of APT-related activity</li> </ul> The Vendor must submit an example of such report as part of submission. |  |
| <b>2</b> | <b>Quality</b>  |  |
| 2.1      | The proposed Vendor solution shall have a robust process in identifying, collecting, analysing, producing, reviewing, and tracking cyber threat information to produce threat intelligence that are relevant to SOC/DST. The proposed Vendor solution shall provide the process stated above as part of the submission  |  |
| 2.2      | The proposed Vendor solution shall categorize the cyber threat intelligence for easy searching and reporting by category. The proposed Vendor solution shall state its categorization supported in the submission   |  |
| 2.3      | The proposed Vendor solution shall enrich the cyber threat intelligence by adding context (Summary Report). The proposed Vendor solution shall state what enrichment is provided in the submission.   |  |
| <b>3</b> | <b>Accuracy</b>   |  |
| 3.1      | The proposed Vendor solution shall provide cyber threat intelligence that is accurate and relevant. The proposed Vendor solution shall provide information on accuracy and relevancy in the submission  |  |
| 3.2      | The proposed Vendor solution shall provide a confidence level for cyber threat information provided. The proposed Vendor solution shall provide information on the confidence level in the submission   |  |
| 3.3      | The proposed Vendor solution shall fine-tune the accuracy of the collection based on feedback from customer   |  |
| <b>4</b> | <b>Timeline</b>   |  |
| 4.1      | The proposed Vendor solution shall provide cyber threat intelligence in a timely manner. The proposed Vendor solution shall provide the tailored intelligence within 24 hours of first exposure to the public   |  |
| 4.2      | The proposed Vendor solution shall provide email alerts when new threat intelligence is available, based on rules configured  |  |
| 4.3      | The proposed Vendor solution should provide multiple different attacks performed by a Cybercriminal or Nation-State group in single place for easy searching and IOCs consumption.  |  |
| <b>5</b> | <b>Research Analyst Access</b>  |  |
| 5.1      | The proposed Vendor solution shall be supported by a research team with good track records with at least 5+ years of experience. The proposed Vendor solution shall demonstrate its track record as part of submission  |  |

|          |   |  |
|----------|---|--|
| 5.2      | The proposed Vendor solution shall be able to provide threat information (sanitized) from its incident response engagements (e.g., victim intelligence)   |  |
| 5.3      | The proposed Vendor solution shall provide analyst access to SOC/DST, for the purpose of additional information request relating to cyber threats, such as threat actor, profiles, tactics, targets etc   |  |
| <b>6</b> | <b>Machine Readable Technical Threat Intelligence (Feed)</b>  |  |
| 6.1      | The proposed Vendor solution shall provide Indicator of Compromise (IoC) information in machine readable format. IoCs shall include both network and host-based indicators. The proposed Vendor solution shall provide the types of IoCs provided in the submission   |  |
| 6.2      | The proposed Vendor solution shall support STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) and CSV format. The proposed Vendor solution shall state other formats supported in the submission  |  |
| 6.3      | The proposed Vendor solution shall maintain and update the list of IoCs provided to SOC/DST   |  |
| 6.4      | The proposed Vendor solution shall provide IoC machine readable format that is supportable by the SOC/DST 's SIEM platform. The proposed Vendor solution shall support SOC/DST in configuring the SOC/DST 's SIEM platform to pull down IoC information automatically as part of the onboarding   |  |
| 6.5      | The proposed Vendor solution shall provide option to access the cyber threat intelligence via REST API. The proposed Vendor solution shall state if the information provided via the REST API is structured or unstructured   |  |
| 6.6      | The proposed Vendor solution shall state out-of-box support for Cyber Threat Intelligence Platform ("TIP") from reputable proposed Vendor solutions. The proposed Vendor solution shall state what TIP platform it supports out-of-box as part of the quotation submission  |  |
| <b>7</b> | <b>Portal</b>   |  |
| 7.1      | The proposed Vendor solution shall provide a portal for SOC to view and access the threat information knowledge base.   |  |
| 7.2      | The proposed Vendor solution portal shall provide search features for SOC/DST to search based on keywords, IP addresses, file hashes, threat actors, malware names, CVE et cetera. The search should preferably support complex searches such as AND, OR search expressions. The proposed Vendor solution shall state the search capabilities as part of quotation submission |  |
| 7.3      | The proposed Vendor solution portal shall provide capabilities to alert SOC/DST for any new relevant content made available. The proposed Vendor solution shall state the different customizations supported to configure the alerting feature  |  |
| 7.4      | The proposed Vendor solution portal shall provide periodic summary via email. The proposed Vendor solution shall state what are the regular finished threat intelligence products included as part of the proposal.   |  |
| <b>8</b> | <b>Threat Briefing</b>  |  |
| 8.1      | The proposed Vendor solution shall provide regular threat calls to brief its customers on strategic cyber threat outlook and round-up. The proposed Vendor solution shall state the format and structure of such threat calls in the submission on request  |  |

|           |   |  |
|-----------|---|--|
| 8.2       | The proposed Vendor solution shall provide periodic threat landscape briefing to its customers. The proposed Vendor solution shall state the format and structure of such threat landscape briefings in the quotation submission  |  |
| <b>9</b>  | <b>Post Implementation Support</b>  |  |
| 9.1       | The proposed Vendor solution shall provide First Level Support for post implementation  |  |
| 9.2       | The proposed vendor must provide 24x7 access to analyst team via portal to provide support on various types of RFIs such as - Phishing Take down, Threat Actor Profiling, IOCs enrichment, Malware reverse engineering, email and APK analysis etc                                      |  |
| 9.3       | The proposed Vendor solution must maintain history of all the requests or tickets on the portal for search and follow ups.  |  |
| 9.4       | Provide SOC/DST with regular updates of its key innovations and capabilities, as well as market intelligence on related products and services that the proposed Vendor solution is providing SOC/DST, and providing business or technical consultancy service to SOC/DST as appropriate |  |
| 9.5       | Proposed Vendor solution is to provide an individual who will be the primary contact for SOC/DST at the regional and local country level. This representative will:   |  |
| 9.6       | Have overall responsibility for managing and coordinating the proposed Vendor solution's services   |  |
| 9.7       | Meet regularly with SOC/DST representative and our appointed third-party proposed Vendor solutions if required  |  |
| 9.8       | Have the authority to make decisions with respect to actions to be taken by proposed Vendor solution in the ordinary course of day-to-day management of SOC/DST 's account  |  |
| 9.9       | Ensuring internal compliance to SOC/DST 's stated process and procedures  |  |
| <b>10</b> | <b>Service Provider Credibility</b>   |  |
| 10.1      | Service provider must have at least 10 years of experience in Cyber Threat Intelligence and forensic investigations related to cyber security across various countries (at least 5 countries)   |  |
| 10.2      | Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorised by specific APT groups.   |  |
| 10.3      | Service provider must release at least 5 reports publicly in a year covering High-tech crimes by different Threat Actor groups providing technical details of attacks and TTPs.   |  |
| 10.4      | The service provider must have their own Computer Security Incident Response Teams (CSIRTs) accredited by an external agency.   |  |
| 10.5      | Service provider must be member of at least 2 of reputed industry institutions such as FIRST/TRUSTED INTRODUCER/APWG  |  |
| 10.6      | The service provider shall be in "Market Guide for Digital Forensics and Incident Response Services" by Gartner as a Representative Vendor  |  |
| 10.7      | The service provider must have been recognised by some industry experts/analysts for their Cyber Threat Intelligence services such as – Cybersec Asia, Cyber excellence, Forrester and Frost & Sullivan for APAC region.  |  |

|      |   |  |
|------|---|--|
| 10.8 | Service provider must have in-house capabilities to engage with law enforcement agencies and CERTs of different countries to provide assistance in investigations. Please provide public reference case studies of your engagement with law enforcement agencies. |  |
|------|---|--|

### 5.5 Video Wall

| S.No | Parameters                      | Minimum Technical Requirements   | Compliance (Y/N) |
|------|---------------------------------|--|------------------|
| 1    | Configuration                   | Video Wall cubes of 70"( $\pm 5\%$ ) diagonal in a 4(C) x 2(R) configuration complete with base stand  |                  |
| 2    | Cube & Controller               | Cube & controller, Software should be from same OEM  |                  |
| 3    | Native Resolution               | Full HD (1920x 1080)   |                  |
| 4    | Light Source                    | Laser light source with a minimum lifetime of 100000 hrs. Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen  |                  |
| 5    | Brightness of Projection engine | 2000 Lumens or better  |                  |
| 6    | Brightness of Cube              | Minimum 800 cd/m <sup>2</sup> and should be adjustable for lower or even higher brightness requirements.   |                  |
| 7    | Brightness Uniformity           | minimum 98 % (ANSI 9) Automatic and continuous calibration system should be provided to maintain uniformity in color and brightness using integrated color sensor  |                  |
| 8    | Dynamic Contrast                | 500000:1 or more   |                  |
| 9    | Dust Prevention                 | Should be designed to prevent dust entering the engine   |                  |
| 10   | Heat dissipation                | Maximum 955 BTU/Hr in normal mode or less  |                  |
| 11   | Pixel clock                     | 165 MHz or higher  |                  |
| 12   | Control                         | IP Based control or IR Based   |                  |
| 13   | Remote                          | IR remote control or IP based control should also be provided for quick access   |                  |
| 14   | Screen to Screen Gap            | < 1 mm Gap between 2 screens   |                  |
| 15   | Screen Support                  | screen should not be expanding or shrinking due to variations in humidity and temperature or any other climatic conditions   |                  |
| 16   | Control BD Input terminals      | Minimum one port of DVI/HDMI/Display Port. All ports should be future ready to take 4HD input  |                  |
| 17   | Power Consumption               | Power Consumption for each VDU/Rear Projection Modules should be less than 280 Watts in normal mode  |                  |
| 18   | Power Supply                    | 100 – 240 VAC, 50-60Hz   |                  |
| 19   | Cooling Inside Cube             | Any advanced cooling mechanism   |                  |
| 20   | Cube Depth                      | 1000 mm or less, Video Wall Design should be trapezium in shape to protect it from falling in any way, Projector should be light-weight single assembly easy to replaceable on-site  |                  |
| 21   | Laser Bank                      | Multiple redundant LASER Banks in the projector  |                  |
| 22   | Noise Level                     | < 35 dB  |                  |
| 23   | Maintenance Access              | Cube should be accessible from the rear side for maintenance.  |                  |
| 24   | Cube control & Monitoring       | Video wall should be equipped with a cube control & monitoring system. It should provide options to view remotely<br>Should be able to control & monitor individual cube, multiple cubes and multiple video walls<br>Should provide a virtual remote on the screen to control the video wall<br>Status log file should be downloadable as per user convenience |                  |

| S.No                         | Parameters              | Minimum Technical Requirements  | Compliance (Y/N) |
|------------------------------|-------------------------|---|------------------|
| 25                           | Sharing & Collaboration | It should be possible to share the layouts over LAN/WAN Network with Display in Meeting room or on Remote Workstations connected on LAN/WAN Network   |                  |
| <b>Video Wall Controller</b> |                         |   |                  |
|                              | Parameters              | Minimum Specification Descriptions  | Compliance (Y/N) |
| 27                           | CPU                     | Intel® Xeon® Octa core 2.1 GHz Processor (3.0GHz max. Turbo frequency)  |                  |
| 28                           | Memory                  | min. 32 GB RAM and expandable up to 64 GB   |                  |
| 29                           | Hard Disk               | R.A.I.D-1 redundant setup with 2x 1000GB 2.5" HDD Hard disk   |                  |
| 30                           | Cooling                 | Should be equipped with dual FAN for cooling  |                  |
| 31                           | Network                 | 2x 1Gb/s LAN  |                  |
| 32                           | System backplane        | Min. 7x slot PCI Express backplane  |                  |
| 33                           | Outputs                 | Up to 8 HD displays   |                  |
| 34                           | Graphics Card           | 4ch Graphic card  |                  |
|                              |                         | Max resolution:<br>3840x2160@60Hz   |                  |
| 35                           | Operating System        | Windows 10 64-bit IoT Enterprise  |                  |
| 36                           | Tampering Alarm         | Controller cover opening alarm  |                  |
| 37                           | Output                  | DP/DVI/HDMI   |                  |
| 38                           | Input                   | H.264, MPEG2/4, MxPEG, MJPEG, V2D, H.263  |                  |
| 39                           | Dimensions              | 19" Rack mount  |                  |
| 40                           | Operating Conditions    | 100-240V ,10-5A, 50/60Hz, Redundant Power supply  |                  |
| 41                           | Operating Temperature   | 0° to 40°C   32° to 104°F   |                  |
| 42                           | Humidity                | Max. 80% Rh(noncondensing) @ 40°C   |                  |
| 43                           | Noise Level             | Max. 50dbA (measured at 1m/3.28ft distance at 22°C/72°F)  |                  |
| 44                           | Regulation Compliance   | UL, CB, BIS, FCC, CE, IEC 60950, IEC 62368  |                  |
| 45                           | Wireless                | The operator should be also possible to show Laptop Or Android/IoS phone over the video wall without disturbing the existing network over wireless  |                  |
| 46                           | Software                | The software should be able to preconfigure various display layouts and access them at any time with a simple mouse click or schedule/timer based.  |                  |
| 47                           | Software                | The software should be able display multiple sources anywhere on video wall in any size.<br>Key features of Video Wall management Software  |                  |
|                              |                         | <ul style="list-style-type: none"> <li>Central configuration database</li> <li>Browser based user interface</li> <li>Auto-detection of network sources</li> <li>Online configuration of sources, displays and system variables</li> </ul>   |                  |
| 48                           | Software                | Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes:   |                  |
|                              |                         | <ul style="list-style-type: none"> <li>Switching the entire display wall on or off.</li> <li>Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules.</li> <li>Fine-tune colour of each cube</li> </ul> |                  |
| 49                           | Software                | Should support Multiple clients / Consoles to control the Wall layouts  |                  |
| 50                           | Software                | The Software should be able to share layouts b/w available different videowalls on same network as well as preview of sources on the workstation  |                  |
| 51                           | Software                | Software should enable the user to display multiple sources (both   |                  |



| S.No | Parameters | Minimum Technical Requirements   | Compliance (Y/N) |
|------|------------|--|------------------|
|      |            | local & remote) up to any size and anywhere on the display walls (both local & remote).  |                  |
| 52   | Software   | The software should be able to create layouts and launch them as and when desired  |                  |
| 53   | Software   | The Display Wall and sources (both local & remote) should be controlled from Remote PC through LAN without the use of KVM Hardware.  |                  |
| 54   | Software   | Software should support display of Alarms  |                  |
| 55   | Software   | The software should provide at least 2 layers of authentication  |                  |
| 56   | Software   | Software should be able to Save and Load desktop layouts from Local or remote machines   |                  |
| 57   | Software   | All the Layouts can be scheduled as per user convince.<br>Software should support auto launch of Layouts according to specified time event by user   |                  |
| 58   | Software   | It should be possible to create layouts comprising of screen scrapped content of Workstations, DVI inputs, Web sources, URLs configured as sources. Layouts can be pre-configured or changed in real time<br>Can be pre-configured or changed in real time   |                  |
| 59   | Software   | It should be possible to schedule specific Layout based on time range<br>It should be possible to share the layouts over LAN/WAN Network with Display in meeting room or on Remote Workstations connected on LAN/WAN Network   |                  |
| 60   | Software   | System should have a quick monitor area to access critical functions of the video wall User should be able to add or delete critical functions from quick monitor area<br>Full featured Web services-based API supports Legacy RS-232 and TCP/IP<br>All software communication should be encrypted, Secure user Management with AD and LDAP Support<br>Zero Maintenance, automatically saves the user's work |                  |
| 61   | Software   | Integrated Embedded & External Audio formats with Audio decoding of video streams also possible<br>Software also supports UMD, IDC, Source name, Time (time zone aware), Date, text, Logo, Message Ticker, Source Status   |                  |
| 62   | Software   | The system shall include complete Bi-directional Soft KVM to permit operators to take mouse & keyboard control of Displays, Screen Scrapped applications and DVI source  |                  |
| 63   | Software   | It should be possible to create two separate Tickers which run concurrently. These can be positioned at top or bottom and can run independently. The Ticker can be picked from data source through screen scrapping or through typing specific incidence, manually   |                  |
| 64   | Software   | The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet   |                  |
| 65   | Software   | The control of the wall shall be possible via a network. All cubes shall have their own IP address, and the control software can access all of them at the same time. The available features shall be: On/Off, Brightness and Colour, Input control<br>Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Colour, Input control, health monitoring.                       |                  |

| S.No | Parameters | Minimum Technical Requirements  | Compliance (Y/N) |
|------|------------|---|------------------|
|      |            | Also, software have feature to show maximum, minimum, and current brightness / colour values of all the projectors.   |                  |
| 66   | Software   | Central setup & Connection management, Central configuration database, fully distributed & modular component technology, Browser based UI, Auto-detection of network sources  |                  |
| 67   | Software   | Online configuration of sources, backup & restore, scheduled backup, fully features web services based API covering all legacy and encrypted communications   |                  |
| 68   | Software   | Save and load layouts (complete display presets including perspectives and applications), start stop and position applications & sources freely over the complete desktop, remote keyboard and mouse control from and towards other networked desktops (bi-directional) |                  |
| 69   | Software   | Supported sources:<br>Analog & digital / streaming video, Analog (RGB) and Digital (DVI-I) Sources, Network desktops, Network multi-channel workstations and applications, Internet & internet sources, Embedded & external audio formats, Localization                 |                  |
| 70   | Modules    | The Display Modules, Display Controller & Software should be from a single OEM  |                  |

#### 5.6 Workstation with dual monitor

| S.No | Parameters        | Parameter and Minimum Specification  | Compliance (Yes/No) |
|------|-------------------|--|---------------------|
| 1    | Processor         | Minimum latest generation i5 or Higher   |                     |
| 2    | Motherboard       | OEM Motherboard  |                     |
| 3    | RAM               | Minimum 8 GB DDR3 RM expendable to 32 GB   |                     |
| 4    | Graphics card     | Minimum Graphics card with 2 GB video memory (non- shared)   |                     |
| 5    | Monitor           | Monitors of 24" TFT LED monitor, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, 1xDVI, Energy star 5.0/BEE star certified |                     |
| 6    | HDD               | Min. 500 GB SSD Drive  |                     |
| 7    | Other Accessories | Line/Mic IN, Line- out/Spr Out (3.5 mm), Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse,   |                     |
| 9    | Operating System  | 64-bit pre-loaded OS with recovery disc  |                     |

#### 5.7 Hardware, Tools, Resources Requirement

Bidder Need to submit the hardware sizing as below table along with Bid , Bidder will provision the Hardware. Any other Item like OS, DB licenses requirement need to be factored by Bidder along with SIEM and SOAR Software cost. Bidder will provide all required software license from day 1.

| S. No. | Application Name | Physical/VM | No. of Instance | vCPU per VM | Memory/VM | OS Storage (GB) | External Storage (TB) | Total External Storage (TB) | Disk type for External Storage | OS Details | Database Software if any | HA Required ? | Remarks |
|--------|------------------|-------------|-----------------|-------------|-----------|-----------------|-----------------------|-----------------------------|--------------------------------|------------|--------------------------|---------------|---------|
|--------|------------------|-------------|-----------------|-------------|-----------|-----------------|-----------------------|-----------------------------|--------------------------------|------------|--------------------------|---------------|---------|

## Section IV: Service Level Agreement (SLA), Penalties & Payment Terms

### 1.1. Implementation Timeline & Penalties:

| S/N | Measurement  | Target  | Penalty for Delay  |
|-----|--|---|--|
| 1   | Kick-off meeting   | 2 weeks from issuance of Lol/ Award of Contract | Rs 50,000/week or part thereof. Delay Beyond 4 weeks, SOC/DST may terminate the contract and Forfeit the PBG.  |
| 2   | Supply of all Components (Hardware, Software, License, etc.)                         | T1 = T + 8 weeks                                | A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T + 10 weeks SOC/DST may terminate the contract and Forfeit the PBG |
| 3   | Installation and Commissioning of all Components (Hardware, Software, License, etc.) | T2 = T1 + 4 weeks                               | A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T1 + 6 weeks SOC/DST may terminate the contract and Forfeit the PBG |
| 4   | Final Acceptance Test (Go-Live of the Project)                                       | T3 = T + 14 weeks                               | A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T2 + 4 weeks SOC/DST may terminate the contract and Forfeit the PBG |
| 5   | Deployment of manpower proposed for O&M of SOC                                       | Within 15 days of successful FAT                | Rs. 20,000/- per individual manpower / per week of delay. To be measured on pro-rata basis as per deployment of manpower. Delay beyond T3 + 3 weeks SOC/DST may terminate the contract and Forfeit the PBG                 |

T = Date of Award of Contract

### 1.2. Service Level Agreement & Penalties

1.2.1. The Successful Bidder is required to execute a Service Level Agreement with SOC/DST covering all terms and conditions of this tender. Bidders need to strictly adhere to the Service Level Agreements (SLA). Services delivered by the bidder should comply with the SLA mentioned in the table below and the scope of services mentioned herein above. SLA will be reviewed on a quarterly basis

| S No. | Service Area                           | Service Level   |
|-------|--|---|
| 1.    | SOC Monitoring & Log Analysis Services | <ul style="list-style-type: none"> <li>• 24x7 event / log monitoring and correlation of the assets in Scope.</li> <li>• 24x7 monitoring of the Database Activity using a Database Activity monitoring tool which directly integrated with the SIEM solution.</li> <li>• 24x7 Monitoring &amp; recording of Security events at all the ingress points.</li> <li>• Event alerts within 15 minutes of the event</li> <li>• Mitigation of security events / threats</li> <li>• Availability of relevant logs for last 3 months</li> <li>• Real time dashboard view</li> </ul> |

|    |                                     |  |
|----|-------------------------------------|--|
|    |                                     | <ul style="list-style-type: none"> <li>• Monthly consolidated report by 5th of every month</li> <li>• Quarterly Reports</li> <li>• Standard / Exception reports</li> </ul>   |
| 2. | Security Intelligence feed Services | <ul style="list-style-type: none"> <li>• Validation of advisories within 12 hours of new global threats &amp; vulnerabilities disclosures.</li> </ul>  |
| 3. | Reports & Dashboard                 | <ul style="list-style-type: none"> <li>• SOC should provide daily / weekly / monthly / quarterly reports for each of the services in a timely manner.</li> <li>• Dashboard should give online view of all devices monitored with their status</li> </ul>   |
| 4. | Others                              | <ul style="list-style-type: none"> <li>• Bidder should provide up-to-date contacts and Escalation matrix.</li> <li>• The Bidder should procure a reputed commercial tools / software's for SOC.</li> <li>• Availability of operation staff on 24/7 basis.</li> <li>• Rule-based Review of Firewalls</li> </ul> |

| Sl. No. | Definition                              | Measurement Interval | SLA Target                                      | Penalty terms  |
|---------|---|----------------------|---|--|
| 1.      | Device uptime / Device availability     | Monthly              | >=99.90%  | >=99.90% No Penalty  |
|         |   |                      |   | >=98.00% and <99.90%<br>0.5% of QGR value  |
|         |   |                      |   | >=95.00%; < 98.00%<br>1% of QGR value  |
|         |   |                      |   | <95.00%<br>1% of QGR value for every percentage drop   |
| 2.      | SOC application / software availability | Monthly              | >=99.90%  | >=99.90% No penalty  |
|         |   |                      |   | >=98.00%; <99.90% 0.5% of QGR value  |
|         |   |                      |   | >=95.00%; < 98.00% 1% of QGR value   |
|         |   |                      |   | <95.00% 1% of QGR value for every percentage drop  |
| 3.      | Manpower availability                   | Monthly              | 100% attendance as per defined in RFP document. | Resource replacement with equivalent skills and experience / with approval from department – no penalty. |
|         |   |                      |   | Level 1 resource absent: Equal cost of the resource proposed by the bidder per day on pro rata basis.    |
|         |   |                      |   | Level 2 resource absent: Double the cost proposed by the bidder per day on pro rata basis.               |
|         |   |                      |   | Level 3 resource absent: 0.1% of QGR value.  |

## 1.2.2. Operational SLAs

| SLA Definition             | Metric                              | Severity  | SLA              | Measurement | Penalty                                    |
|----------------------------|-------------------------------------|-----------|------------------|-------------|--|
| Incident Management        | Incident Response Time              | Level 4   | 15 minutes       | Quarterly   | Rs. 7000/hour for every hour of delay      |
|                            |                                     | Level 3   | 30 minutes       | Quarterly   | Rs. 5000/hour for every hour of delay      |
|                            |                                     | Level 2   | 3 hours          | Quarterly   | Rs. 2000/hour for every hour of            |
|                            |                                     | Level 1   | 6 hours          | Quarterly   | Rs. 1000/hour for every hour of delay.     |
|                            | Incident Resolution Time            | Level 4   | 4 hours          | Quarterly   | 2% of QGR value for every hour of delay.   |
|                            |                                     | Level 3   | 8 hours          | Quarterly   | 1% of QGR value for every hour of delay.   |
|                            |                                     | Level 2   | 2 days           | Quarterly   | 0.5 % of QGR value for every day of delay. |
|                            |                                     | Level 1   | 4 days           | Quarterly   | Rs. 10000/day for every day of delay.      |
| Service Request Management | SOC Tool Rules Update               | Emergency | 4 Hrs            | Quarterly   | 1% of QGR value for every hour of delay    |
|                            |                                     | Normal    | 2 days           | Quarterly   | 1% of QGR value for every day of delay     |
|                            | Vulnerability Scan                  | Emergency | 4 hrs            | Quarterly   | 2% of QGR value for every hour of delay    |
|                            |                                     | Normal    | 2 days           | Quarterly   | 1% of QGR value for every day of delay     |
|                            | SOC Operations Effectiveness Review |           | Once in 3 Months | Yearly      | 2% of QGR value for every delay            |
|                            | SOC Architecture Review             |           | Once in a year   | Yearly      | 2% of QGR value for every delay            |

## 1.2.3. Supply, Installation, Commissioning

- All the items as mentioned in the BOM should be supplied, delivered, and commissioned within the mentioned timelines. Any delay would attract penalty.
- In case only some items of BOM are not as per timelines, then penalty would calculate on pro-rata basis item wise.
- The date of commissioning would be considered the date when a written communication would be sent by the bidder to DST for FAT readiness

**Note:**

Root Cause should be identified for all incidents, if root cause is not identified then additional penalties will be levied.

**The security breach** will include but not limited to successful penetration of any Virus, Trojan, malwares, zero-day attacks, intrusion, Denial of Service Attacks, ...etc., up to the Server level. In case of any compromise of data due to the Security Breach then double penalty will be levied.

**1.3. Payments Schedule**

| S/N                         | Activity  | Payment (%)   |
|-----------------------------|---|---|
| <b>Table 1: Schedule-I</b>  |   |   |
| 1                           | Delivery of all components (Hardware, Software, Licenses, etc.) at SOC, Gandhinagar   | 70% of the sum total of schedule I of financial bid   |
| 2                           | Successful installation, Testing, Integration, Commissioning  | 10% of the sum total of schedule I of financial bid   |
| 3                           | Successful completion of training & Final Acceptance test of entire solution  | 20% of the sum total of schedule I of financial bid   |
| <b>Table 2: Schedule-II</b> |   |   |
| 1                           | 5 Years CAMC/warranty and Back-to-Back OEM support and Operation & Maintenance costs including manpower for the entire Infrastructure | Will be divided and paid in 20 equal Quarterly Installments after the end of each quarter (3 months).<br>Five years will start from the date of successfully completion of FAT. |