Bid Number: GEM/2023/B/4096001
Dated: 21-11-2023

Bid Corrigendum

GEM/2023/B/4096001-C4

Following terms and conditions supersede all existing “Buyer added Bid Specific Terms and conditions” given in the bid document or any previous corrigendum. Prospective bidders are advised to bid as per following Terms and Conditions:

Buyer Added Bid Specific Additional Terms and Conditions

1. OPTION CLAUSE: The Purchaser reserves the right to increase or decrease the quantity to be ordered up to 25 percent of bid quantity at the time of placement of contract. The purchaser also reserves the right to increase the ordered quantity by up to 25% of the contracted quantity during the currency of the contract at the contracted rates. Bidders are bound to accept the orders accordingly.
2. Data Sheet of the product(s) offered in the bid, are to be uploaded along with the bid documents. Buyers can match and verify the Data Sheet with the product specifications offered. In case of any unexplained mismatch of technical parameters, the bid is liable for rejection.
3. IT equipment shall be IPv6 ready from day one.
4. Malicious Code Certificate:

   The seller should upload following certificate in the bid:-
   (a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to :-
   (i) Inhibit the desires and designed function of the equipment.
   (ii) Cause physical damage to the user or equipment during the exploitation.
   (iii) Tap information resident or transient in the equipment/network.
   (b) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.
5. **Manufacturer Authorization:**Wherever Authorised Distributors/service providers are submitting the bid, Authorisation Form /Certificate with OEM/Original Service Provider details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid
6. Bidders can also submit the EMD with Account Payee Demand Draft in favour of
   Indian Statistical Institute
   payable at
   Kolkata
   .
   Bidder has to upload scanned copy / proof of the DD along with bid and has to ensure delivery of hardcopy to the Buyer within 5 days of Bid End date / Bid Opening date.
7. Successful Bidder can submit the Performance Security in the form of Account Payee Demand Draft also (besides PBG which is allowed as per GeM GTC). DD should be made in favour of
   Indian Statistical Institute
   payable at
   Kolkata
   . After award of contract, Successful Bidder can upload scanned copy of the DD in place of PBG and has to ensure delivery of hard copy to the original DD to the Buyer within 15 days of award of contract.
8. Bidder's offer is liable to be rejected if they don't upload any of the certificates / documents sought in the Bid document, ATC and Corrigendum if any.
9. Availability of Service Centres: Bidder/OEM must have a Functional Service Centre in the State of each Consignee's Location in case of carry-in warranty. (Not applicable in case of goods having on-site warranty). If service center is not already there at the time of bidding, successful bidder / OEM shall have to establish

one within 30 days of award of contract. Payment shall be released only after submission of documentary evidence of having Functional Service Centre.

10. Buyer Added text based ATC clauses

Scope of Work

(i) To supply, install, configure, integrate, commission and provide support of Email Security Gateway solution to meet the requirements of the project for 3 years post Go-Live.

(ii) The solution shall be implemented at the CSSC at Indian Statistical Institute (ISI), Kolkata.

(iii) The supplied system should be integrated with other parts of email delivery pipeline and security appliances of ISI-Kol IT infrastructure.

(iv) Bidder should carry out the security hardening of the supplied components, including but not limited to hardware, software, and application. The hardening should be in conformance with the standard security guidelines of ISI-Kol.

(v) Bidder should ensure engagement of OEM during the implementation and maintenance period and should submit proof of warranty and 24x7 enterprise support with the OEM agreement executed in the name of ISI-Kol exclusively for this project. There shall be no limitations on the enterprise support.

(vi) Bidder should undertake to conduct Quality Assurance testing and assist ISI-Kol to perform User Acceptance Testing.

(vii) Bidder should provide post-implementation training to ISI-Kol officials for regular management and operation purpose.

(viii) Bidder should deliver all the relevant documents, SOPs required for the smooth implementation and operation of the project before final acceptance. The documents and design should be vetted by the respective OEMs.

(ix) Bidder should provide post-implementation support for the offered systems by trained support engineers.

(x) The selected vendor is expected to close all the vulnerabilities/weakness identified by ISI-Kol in a time bound manner during implementation and warranty period.

(xi) The selected vendor is expected to comply with all the security policies of ISI-Kol before acceptance of Final solution.

(xii) Full documentation, SOPs of the project are to be included in the deliverables by the successful Vendor.

(xiii) The selected vendor should integrate with ISI-Kol’s existing NTP server for setting the global time settings.

(xiv) The successful vendor will be expected to provide all the necessary software licenses, implement, train and handover the solution to ISI-Kol officers. The bidder would subsequently provide support through bug fixes, updates, and upgrades, troubleshooting, configuration changes, etc., by visiting ISI-Kol premises as and when required.

(xv) All the supplied systems should be covered under onsite warranty for 3 years from post Go-Live date.

(xvi) The solution provider should perform migration of data from the existing solution to the new supplied solution. The data for the migration includes policies, rules etc. of the existing email gateway solution.

(xvii) ISI-Kol may further extend the quantity to additional user licenses for all the prop osed products/ solutions at the same rate as and when required during the contract pe riod.

(xviii) In case of any conflict between the GeM defined Catalogue Specification/ Terms & Conditions & those mentioned in ATC specified by the procuring entity, the details gi ven in ATC will prevail. Technical Evaluation will be done as per the conditions of ATC document.

Additional terms and conditions

1. The offered product specification should be as per the specification mentioned in **Annexure-1** and no dev iation from it will be accepted. Compliance of BoQ Specification as per Annexure-1 must be submitted.

2. The bidder must provide complete technical compliance documentation in accordance with the specified t echnical requirements. Furthermore, the technical compliance documentation should be accompanied by a product datasheet or brochure, which should be publicly accessible on the OEM's website for verification pur poses. Website link of the product line and datasheets, which may provide necessary evidence(s), must be p rovided.

3. Manufacturer Authorization Certificates from the OEM mentioning the specific Bid Number should be sub mitted for the proposed solution, failing which the bid will be rejected.

4. The OEM of the proposed solution should be an established and reputable company with a minimum of 10 years of experience within the cybersecurity sector. Bidder should submit a publicly verifiable list of such pro ducts which may show presence of the OEM for said amount of time.

5. OEM should be a reputed email security gateway vendor with a **market presence in India for at least the last 5 years,** with both hardware appliance-based and virtual appliance-based solutions. OEM must hav e 24x7 online Technical Support available (details to be provided). OEM should have supplied at least 5 emai l gateway solutions in the last 3 years in India and PO copies with contact information of such clients should be provided with the bid.

6. The OEM must also have a proven track record in effectively identifying vulnerabilities within software sys tems. Documentary evidence of list of such publicly available reports may be provided as necessary evidenc e(s).

7. To demonstrate their expertise in threat research, the OEM should maintain a research team that has pub lished a minimum of **20 technical documents in the past two years,** specifically in areas related to cyb ersecurity. Documentary evidence of list of such publicly available documents may be provided as necessary evidence(s).

8. Additionally, the OEM should receive data feeds from its own threat intelligence platform, ensuring reasonable visibility and presence in the global digital landscape. Documentary evidence mentioning the name of the platform along with website link and publicly available datasheets/ reports which may be provided as necessary evidence(s).

9. The Bidder must have a registered office in Kolkata. Documentary evidence issued by any Govt. agency to this effect must be submitted.

10. The OEM of the Proposed solution should be among the top 10 players in last 3 published email security gateway reports by Gartner/ Radicati. Website reference of such list, may be provided as necessary evidence(s).

11. Bidder must have been engaged in IT-related services at least for the last 3 years and must have supplied at least 1 email gateway solution in the last 3 years. PO copy to be submitted.

12. The bidder should submit the Make In India Declaration as per the Annexure-2 enclosed herewith.

13. There will be a Pre-Bid Meeting to be held on 01.11.2023 in Hybrid mode. Bidders may join the meeting physically on 01.11.2023 at 4.00 PM in the following address at the same time they can join the meeting online in following link:

Venue: CE's Conference Room, ISI, 203 BT Road, Kolkata-700108

link: Pre Bid Meeting for Purchase of Email Security Gateway

Wednesday, 1 November · 4:00 – 6:00pm

Time zone: Asia/Kolkata

Google Meet joining info

Video call link: https://meet.google.com/ims-rsdf-uyd

Annexure-1

Specification of Email Security Gateway Solution

S. No.	Item	Details
1	Type of Appliance	Virtual Appliance for on premise deployment. Should be deployable through VMWare (v7.0)
2	Email Gateway	1. It should be able to act as the email gateway for the exchange of emails, on behalf of the institute email domain(s) and should support Simple Mail Transfer Protocol (SMTP) to accept and deliver messages. 2. It should be able to route emails on behalf of multiple domains. 3. It should be able to send multiple messages per connection and open multiple connections per host.

3	No of Users	Should support at least 650 users from Day 1, and extendable up to 1000 users with the purchase of additional user licenses only.
4	Email Encryption	Should support SSL/TLS as well as S/MIME (or equivalent) for encrypted delivery of inbound as well as outbound emails.
5	Email Security	Should support (at least) the following features from Day 1, on the email processing pipeline for both incoming as well as outgoing emails (whenever applicable). 1. The solution should support the ability to perform SMTP session control and traffic rate limiting according to the sender's IP address/range, domain or email reputation. 2. The solution should have a spam catch rate of greater than 99 per cent, with a false-positive rate of less than one in one million. The solution should provide a mechanism to configure Anti-Spam Aggressiveness on a global basis. Performance/efficiency declaration from OEM should be provided on OEM's letterhead, with supporting documentary evidence. 3. Should examine the reputation of the email sender to filter out malicious senders (both domain and hosts). 4. Should analyze email content using a variety of techniques to filter out phishing emails. 5. Should be able to detect and block zero-day malware attacks. Should check for security updates and threat intelligence data updates at least twice a day. 6. Should be able to detect junk emails and filter them (configurable). 7. Should prevent Directory Harvesting, and similar brute-force attacks

S. No.	**Item**	**Details**
		8. Should protect from URL-related attacks (e.g. Time- of-Click) and per-user tracking of Web interaction. Should work for shortened URLs also. 9. Should provide message quarantine (for spam emails, viruses, and outbreak incidents) feature, with a size of at least 1GB. Should provide a mechanism for end-user notification daily, along with access to (actionable) message quarantine, on per user basis. Users should be able to access their quarantined emails individually. The administrator should have access to all quarantined mail. 10. Should support configuring with SPF, DKIM, and DMARC features for the institute email domain. The solution should support policies to sign outgoing emails based on domain keys and allow users to sign by different domain keys based on the sender domain. Full-featured DMARC verification for incoming emails should be done by the solution.

6	Management	1. The solution should support the authentication of users using external RADIUS or LDAP for management purposes. 2. The solution should support the following for system monitoring: - SNMP v2/v3, Syslog
7	IPV6 Support	The solution should be able to exchange emails with IPv6 hosts.
8	Data Loss Prevention	Should support setting up a policy, to prevent Data Loss Prevention.
9	End of Support	Should be at least five years from the date of publication of the tender. Such a declaration should be provided on OEM's letterhead.
10	Maintenance	Should provide 36 months onsite comprehensive OEM warranty including (but not limited to) 24*7 OEM support for technical issues, along with access to software upgrades/bug fixes, threat intelligence feed for all available security engines, knowledge base and online resources, and any other licenses and subscriptions needed for proper operation without any additional cost during the entire warranty period.
11	Licensing	1. All the features described above (S. Nos. 1 - 10) should be available from Day 1. 2. No extra cost can be incurred for system upgrades, bug fixes, licenses, subscriptions etc. during the entire warranty period of 36 months (from the day of installation).

Annexure-2

DECLARATION OF LOCAL CONTENT

Tender No: ..... Dated: .....

To

The Chairperson, Tender Committee

Indian Statistical Institute

203, B T Road, Kolkata- 700108

Subject: Declaration of Local Content-reg.

1. Country of origin of Goods being offered: .....

2. We hereby declare that items offered has.....% local content.

(Clarification for Local content calculation as per OM No: P-45021/102/2019-BE-II-Part (1) (E-50310), dated 4th March 2021 of Department of Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Govt. of India.)

3. The details of location(s) at which local value addition is made are given in the below table:

Sl. No.	Name of the item	Location(s) of local value addition

“Local Content” means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured (excluding net domestic indirect taxes) minus the value of the imported content in the item (including all customs duties) as a proportion of total value, in percent.

Important:

“False declaration will be breach of Code of Integrity under Rule 175(1) (i) (h) of the General Financial Rules 2017 for which a bidder or its successors can be debarred for up to two years as per Rule (iii) of the General Financial Rules 2017 along with such other actions as may be permissible under law”

Date:

Yours faithfully,

Corrigendum –2

Date: 21.11.2023

Based on the pre-bid meeting held on 01.11.2023, committee decided to amend the following terms and conditions:

Page No	Heading	Existing Clause	Amended/ To be read as
Page-9, Annexure-1, Sl. No-1	Additional Terms & Condition	Virtual Appliance for on premise deployment. Should be deployable through VMWare (v7.0)	Virtual Appliance for on-premise deployment. Should be deployable through VMWare (v7.0). Dependency of the appliance on cloud-based resources for some services can be there

Page No-8, Sl. No-5	Additional Terms & Condition	OEM should be a reputed email security gateway vendor with a **market presence in India for at least the last 5 years,** with both hardware appliance-based and virtual appliance-based solutions. OEM must have 24x7 online Technical Support available (details to be provided). OEM should have supplied at least 5 email gateway solutions in the last 3 years in India and PO copies with contact information of such clients should be provided with the bid.	OEM should be a reputed email security gateway vendor with a **market presence in India for at least 3 years,** with both hardware appliance-based and virtual appliance-based solutions. OEM must have 24x7 online Technical Support available (details to be provided). **OEM should have supplied at least 5 email gateway solutions in the last 5 years in India** and PO copies with contact information of such clients should be provided with the bid.
Page No-9, Sl. No-10	Additional Terms & Condition	The OEM of the Proposed solution should be among the top 10 players in last 3 published email security gateway reports by Gartner/ Radicati. Website reference of such list, may be provided as necessary evidence(s).	The OEM of the Proposed solution should be among the **top 15** players in last 3 published email security gateway reports by Gartner/ Radicati. Website reference of such list, may be provided as necessary evidence(s).
Page-10, Annexure-1, Sl. No-5, Point No-10	Additional Terms & Condition	Should support configuring with SPF, DKIM, and DMARC features for the institute email domain. The solution should support policies to sign outgoing emails based on **do main** keys and allow users to sign by different domain keys based on the sender domain. Full-featured DMARC verification for incoming emails should be done by the solution.	Should support configuring with SPF, DKIM, and DMARC features for the institute email domain. The solution should support policies to sign outgoing emails based on **domain** keys and allow users to sign by different domain keys based on the sender domain. Full-featured DMARC verification for incoming emails should be done by the solution.

.

11. Buyer uploaded ATC document Click here to view the file.

Disclaimer

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bid. Any clause(s) incorporated by the Buyer regarding following shall be treated as null and void and would not be considered as part of bid:-

1. Definition of Class I and Class II suppliers in the bid not in line with the extant Order / Office Memorandum issued by DPIIT in this regard.
2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.
3. Publishing Custom / BOQ bids for items for which regular GeM categories are available without any Category item bunched with it.
4. Creating BoQ bid for single item.
5. Mentioning specific Brand or Make or Model or Manufacturer or Dealer name.
6. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
7. Floating / creation of work contracts as Custom Bids in Services.
8. Seeking sample with bid or approval of samples during bid evaluation process.
9. Mandating foreign / international certifications even in case of existence of Indian Standards without specifying equivalent Indian Certification / standards.
10. Seeking experience from specific organization / department / institute only or from foreign / export experience.
11. Creating bid for items from irrelevant categories.
12. Incorporating any clause against the MSME policy and Preference to Make in India Policy.
13. Reference of conditions published on any external site or reference to external documents/clauses.
14. Asking for any Tender fee / Bid Participation fee / Auction fee in case of Bids / Forward Auction, as the case may be.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

*This document shall overwrite all previous versions of Bid Specific Additional Terms and Conditions.

This Bid is also governed by the General Terms and Conditions