भारतीय प्रौद्योगिकीसंस्थानमद्रासचेन्नै 600 036
INDIAN INSTITUTE OF TECHNOLOGY MADRAS Chennai 600 036
भंडार एवं क्रय अनुभाग / STORES & PURCHASE SECTION
Email: adstores@iitm.ac.in
दूरभाष: (044) 2257 8285 / 8287 / 8288 / 8290 फैक्स: (044) 2257 8082
Telephone : (044) 2257 8285/8287/8288/8290 FAX: (044) 2257 8082
GSTIN: 33AAAAI3615G1Z6

P.K. SHEBA SABARI
Assistant Registrar (Stores & Purchase)

Date: 22.01.2024

Tender No. IITM/SPS/Web Application/023/2023-24/SPL

Due Date: 12.02.2024 Before 2.00 p.m.

Dear Sirs,

On behalf of the Indian Institute of Technology Madras, Tenders are invited in two bid system, namely technical and financial bids for:

"Web Application Firewall"

Conforming to the specifications enclosed.

Tender Documents may be downloaded from Central Public Procurement Portal **https://etenders.gov.in/eprocure/app.** Aspiring Bidders who have not enrolled / registered in e-procurement should enroll/register before participating through the website https://etenders.gov.in/eprocure/app. The portal enrolment is free of cost. Bidders are advised to go through instructions provided at "Help for contractors". [Special instructions to the bidders for the e-submission of the bids online through this e-Procurement Portal"].

Tenderers can access tender documents on the website (For searching in the NIC site, kindly go to Tender Search option and type 'IIT'. Thereafter, Click on "GO" button to view all IIT Madras tenders). Select the appropriate tender and fill them with all relevant information and submit the completed tender document online on the website https://etenders.gov.in/eprocure/app as per the schedule attached.

No manual bids will be accepted. All tender documents including Pre-qualification, Technical and Financial bids should be submitted in the E-procurement portal**.**

1	**LAST DATE for receipt of Tender**	**:**	**12.02.2024 before 02.00 p.m.**
	Pre-bid meeting	**:**	The **Pre-bid Meeting** will be conducted via Google Meet on 29.01.2024 **@ 3.30 p.m**. Please see the below link to join the meeting https://meet.google.com/jqu-bejm-ddc Prospective bidders are requested to register their participation by sending an email to adstores@iitm.ac.in, with name/designation of the representative who will attend the meeting along with queries on or before 25.01.2024**.**
	Date & Time of opening of Tender	**:**	**13.02.2024 @ 3.00 p.m.**

GUIDELINES FOR TENDER SUBMISSION IN CENTRAL PUBLIC PROCUREMENT PORTAL (E-PROCUREMENT MODE)			
A	**निविदा की प्रस्तुति /Submission of Tender**	:	As per the directives of Department of Expenditure, this tender document has been published on the Central Public Procurement Portal URL: https://etenders.gov.in/eprocure/app The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal More information useful for submitting online bids on the CPP Portal may be obtained at: https://etenders.gov.in/eprocure/app All tender documents including Technical Bid & Financial Bid should be submitted separately in online CPP portal as per the specified format only. Right is reserved to ignore any tender which fails to comply with the above instructions. **No manual bid submission will be entertained.**
B	**ऑनलाइन बोली जमा के अनुदेश / Instructions for online bid submission**	:	**REGISTRATION** • Bidders are required to enrol on the e-Procurement module of the Central Public Procurement Portal URL: https://etenders.gov.in/eprocure/app by clicking on "Online Bidder Enrolment". Enrolment on the CPP Portal is free of charge. • As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts. • Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal. • Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.) https://eprocure.gov.in/eprocure/app with their profile. • Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse. • Bidder then may log in to the site through the secured log-in by entering their user ID / password and the password of the DSC / eToken.
C	**निविदा दस्तावेज़ की खोज / Searching for tender documents**	:	• There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, organization name, location, date, value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords etc. to search for a tender published on the CPP Portal. • Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective **"My Tender"** folder. This would enable the CPP Portal to intimate the bidders through SMS / email in case there is any corrigendum issued to the tender document. • The bidder should make a note of the **unique Tender ID** assigned to

			each tender, in case they want to obtain any clarification / help from the Helpdesk.
D	**बोली की तैयारी /Preparation of bids**	:	• Bidder should take into account any corrigendum published on the tender document before submitting their bids. • Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid. • Bidder, in advance, should prepare the bid documents to be submitted as indicated in the tender document / schedule and generally shall be in PDF / XLS formats as the case may be. Bid documents may be scanned with 100 dpi with black and white option. • To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GSTIN Details, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use **"My Documents"** area available to them to upload such documents. These documents may be directly submitted from the **"My Documents"** area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.
E	**बोली की प्रस्तुति /Submission of bids**	:	• Bidder should log into the site well in advance for bid submission so that he/she can upload the bid in time i.e. on or before the bid submission date and time. Bidder will be responsible for any delay due to other issues. • The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document. • A standard BOQ format has been provided in **Annexure-C** with the tender document to be filled by all the bidders. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. Bidders are required to download the BOQ file, open it and complete the detail with their respective financial quotes and other details (such as name of the bidder). If the BOQ file is found to be modified by the bidder, the bid will be rejected. • The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission. • The **Tender Inviting Authority (TIA)** will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders due to local issues. • The uploaded tender documents become readable only after the tender opening by the authorized bid openers. • Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details. • Kindly add scanned PDF of all relevant documents in a single PDF file of compliance sheet.
F	**बोलीदाताओं के लिए सहायता / Assistance to bidders**	:	• Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender

			Inviting Authority for a tender or the relevant contact person indicated in the tender. • Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk. The contact number for the helpdesk is [0120-4200462, 0120-4001002, 0120-4001005]
G	**बोलीदाताओं के लिए सामान्य अनुदेश /General Instructions to the Bidders**	:	• The tenders will be received online through portal https://etenders.gov.in/eprocure/app. In the Technical Bids, the bidders are required to upload all the documents in single pdf file. • Possession of a Valid Class II/III Digital Signature Certificate (DSC) in the form of smart card/e-token in the company's name is a prerequisite for registration and participating in the bid submission activities through https://etenders.gov.in/eprocure/app • Digital Signature Certificates can be obtained from the authorized certifying agencies, details of which are available in the web site https://etenders.gov.in/eprocure/app under the "Information about DSC".
H	**बयाना जमा / (ईएमडी)Earnest Money Deposit (EMD)**	:	**I.** EMD of **INR 1,05,000/-** (Rupees One Lakh and Five Thousand only) should be transferred through NEFT/RTGS to the following bank account on or before due date **12.02.2024 before 2:00 p.m.** **a. Name : Registrar IIT Madras** **b. Bank : State Bank of India** **c. Account No. : 10620824305** **d. Branch : IIT MADRAS** **e. IFSC CODE : SBIN0001055** **II.** The EMD will be returned to unsuccessful Bidder(s), after finalization of the tender. The EMD shall be forfeited if any Bidder withdraws the offer before finalization of the tender. **III.** The EMD amount should not be sent through DD. **IV.** Non-submission of EMD details on or before the due date and time will result in rejection of the e-bid. **V.** As per Rule 170 of GFR 2017, exemption of EMD will be given subject to submission of undertaking by the firm seeking such exemption. Copies of relevant orders/ documents regarding such exemption should be submitted along with the tender document. VI. The successful bidder shall submit a **Performance Guarantee of 3%** of the bid amount in the form of Demand Draft in favour of **"The Registrar, IIT Madras"** to be obtained from any commercial bank within 15 (fifteen) days from the date of issue of Order by IIT Madras, which shall be released on expiry/termination of the contract after adjustment of dues, if any without any interest. VII. In case of successful bidder, the EMD will be adjusted towards the Performance Security Deposit on request. The amount of EMD is liable to be forfeited, if the bidder withdraws from the offer after submission of the tender or after the acceptance of the offer and fails to remit the Performance Security Deposit.
I	**तकनीकी बोली पर मार्किंग / Marking on Technical Bid**	:	i. The bidder eligibility criteria (Eligibility Criteria – I &I II), technical specification of the item for this tender is given in **Annexure A**. The Bidders shall go through the bidder eligibility criteria, technical specification and submit the technical bid in the proforma given in **Annexure B** in the tender document along with the supporting documents. ii. The Technical bid should be submitted **in pdf format only through online (e-tender). No manual submission of bid will be entertained.**

			iii. The technical bid should have the page-wise **heading as "Technical Bid" and page no.** in all pages with seal and signature of authorized signatory. The total no. of pages should be mentioned at the last page of the documents. **iv. The technical bid should consist of** a) Document proof for EMD payment b) Technical Compliance sheet as per proforma given in **Annexure -B** c) Document proof for bidder eligibility criteria, technical details along with catalogue / brochure and other technical, commercial terms and conditions.
J	**वित्तीय बोली पर मार्किंग / Marking on Financial Bid**	:	Financial bid (BOQ) should be submitted in the prescribed format given **in Annexure- C** in **xls format** through e-tender only. **No manual or other form of submission of Financial Bid will be entertained**.

निविदा के निबंधन व शर्तें /TERMS AND CONDITIONS OF TENDER	
1	**निविदा की तैयारी /Preparation of Tender:** • The bids **should be submitted through online only in two bid system i.e. Technical Bid and Financial Bid separately**. • The bidder has to submit the tender document duly signed on all pages by an authorized person and his / her full name and status shall be indicated below the signature along with official seal/stamp of the firm. Submission of wrong / forged information / document will be liable to legal action, and rejection of the bid submitted by the firm. • The bids of the agency/firm/company not in possession of valid statutory license / registrations are liable for rejection. • If any relative of the bidder is an employee of the IIT Madras, the name, designation and relationship of such employee shall be intimated to the Registrar, IIT Madras in writing while submitting the bid. • No bidder will be allowed to withdraw / alter / modify the bid during the bid validity period.
2	**निविदा पर हस्ताक्षर /Signing of Tender:** • The Tender is liable to be rejected if complete information is not given therein or if the particulars and date (if any) asked for in the schedule to the Tender are not fully filled in or not duly signed/authenticated. Specific attention is drawn to the delivery dates and terms and conditions enclosed herewith. **Each page of the bids required to be signed and bears the official seal of the Bidders.** • If the bid is submitted by a firm in partnership, it shall be signed (with seal) by all the partners of the firm above their full typewritten names and current addresses or alternatively by a partner holding power of attorney for the firm in which case a certified copy of the power of attorney shall accompany the application. A certified copy of the partnership deed along with current addresses of all the partners of the firm shall also accompany the application. • If a limited company or a corporation makes the application, it shall be signed by a duly authorized person holding power of attorney for signing the application, in which case a certified copy of the power of attorney shall accompany the application. Such limited company or corporation may be required to furnish satisfactory evidence of its existence. The bidder shall also furnish a copy of the Memorandum of Articles of association duly attested by a Notary Public.
3	**वह अवधि जिसके लिए ऑफर खुला रहेगा /Period for which the offer will remain open:** • The Tender shall remain open for acceptance/validity till: **120 days from the date of opening of the tender.** However, the day up to which the offer is to remain open being declared closed holiday for the Indian Institute of Technology Madras, the offer shall remain open for acceptance till the next working day.
4	**कीमत /Prices:** • The prices quoted must be net per unit shown in the schedule and must include all packing and delivery charges loading and unloading and other statutory levies considering all scope of work, terms & conditions

	and as per the Technical bid mentioned in **Annexure A**. • Prices should be inclusive of all. • All conditional tenders will be summarily rejected. • **Quote should be in INR.**
5	भुगतान टीमें **/Payment terms :** 100% Payment will be made only after supply and satisfactory installation.
6	**सुपुर्दगी /Delivery:** Items should be delivered and installed with 60 days from the date of Purchase Order.
7	**वारंटी /Warranty**: 3 years
8	**संस्थापन /Installation:** Installation to be done by the bidder and current setup should be migrated.
10	**निबंधन व शर्तें / Terms and Conditions:** Failure to comply with any of the instructions stated in this document or offering unsatisfactory explanations for non-compliance will likely to lead to rejection of offers.
11	**स्वीकृति का अधिकार / Right of Acceptance:** IIT Madras reserves the right to reject the whole or any part of the Tender without assigning any reason or to accept them in part or full.
12	**स्वीकृति की सूचना /Communication of Acceptance:** Letter of Intimation and acceptance will be communicated by post /email to the successful bidder to the address indicated in the bid.
13	All information including selection and rejection of technical or financial bids of the prospective bidders will be communicated through CPP portal. In terms of Rule 173(iv) of General Financial Rule 2017, the bidder shall be at liberty to question the bidding conditions, bidding process and/or rejection of bids.
14	**बोलीदाता को इस निविदा के साथ जमा करना होगा /Bidder shall submit along with this Tender:** Name and full address of the Banker and their swift code and PAN No. and GSTIN number.
15	**क्षेत्राधिकार /Jurisdiction:** All questions, disputes, or differences arising under, out of or in connection with the contract, if concluded, shall be subject to the exclusive jurisdiction at the place from which the acceptance of Tender is issued.
16	**जुर्माना & परिसमापन क्षति /Penalty & Liquidated Damages / Force Majeure**: • If the selected Bidder fails to complete the due performance of the contract in accordance with the terms and conditions, Institute reserves the right either to cancel the contract or to accept performance already made by the selected Bidder after imposing Penalty on Selected Bidder. A penalty will be calculated on a per week basis and on the same Rate as applicable to Liquidated Damages (LD). In case of termination of the contract, Institute reserves the right to recover an amount equal to 5% of the Contract value as Liquidated Damages for non-performance. • Both Penalty and Liquidated Damages are independent of each other and are applied separately and concurrently. Penalty and LD are not applicable for reasons attributable to the Institute and Force Majeure. However, it is the responsibility of the selected Bidder to prove that the delay is attributable to the Institute and Force Majeure. The selected Bidder shall submit the proof authenticated by the Bidder and Institute's official that the delay is attributed to the Institute and/or Force Majeure along with the bills requesting payment.
17	• The bidder shall certify that the tender document submitted by him / her are of the same replica of the tender document as published by IIT Madras and no corrections, additions and alterations made to the same. If any deviation found in the same at any stage and date, the bid / contract will be rejected / terminated and actions will be initiated as per the terms and conditions.
18	• The bidder should study the tender document, bidder eligibility criteria, and technical specification in detail as given in **Annexure A** before submitting the bid.

19 **बोलीदाता पात्रता मानदंड / Bidder Eligibility CRITERIA:**

Eligibility Criteria - I

1. The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**

2. Only 'Class-I local suppliers' and 'Class-II local suppliers', as defined under DIPP, MoCI Order No. P-45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein, shall be eligible to bid in this tender. Declaration for Class-I / Class-II local suppliers should be submitted in the prescribed proforma format as per **Annexure – E.**

Eligibility Criteria - II

1. Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure – F.**

2. The firm must have an aggregate financial turnover of at least Rs.28 lakhs in the last 3 years i.e. 2019-20,2020-21 and 2021-22 (Should enclose the audited financial statement signed by the Chartered Accountant)

3. The firm should have an experience of supplying, installing, configuring, implementing and maintaining more than 200 websites out of which at least one should be in educational or Research Institute in India in the past 2 years.

   Copies of the document listed below should be submitted as a proof for the above work experience:
   a. Work Order
   b. User performance Certificate from End User certifying that the firm maintains 200 websites is mandatory.

4. The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-G.**

5. The bidder should have a service centre in Chennai for service support. Proof of Office in Chennai should be furnished as documentary evidence (such as valid rental agreement / registration certificate / Certificate of Incorporation etc.)

20 **बोलियों की संख्या और उनका प्रस्तुतीकरण /Number of Bids and their Submission:**

Bids should be submitted **CPP portal. Two bid system** should be followed as detailed below:

Bid I Technical Bid

The bidder should go through the bidder eligibility criteria – I & II and technical specification given in **Annexure-A** of the tender document, understand the requirement of IITM and submit their technical bid along with all relevant document proof in the proforma given in **Annexure–B**. **Any tender documents without these shall be invalid and rejected.**

The technical bid should consist of proof of EMD transfer, Bidder Eligibility Criteria – I & II, Technical specification and compliance sheet (proforma given in **Annexure – B)** along with all relevant documents proof.

Bid II Financial Bid

The financial bid should be submitted as per the proforma (**Annexure C**). The Quoted price should be for supply and installation of the item and inclusive of all cost at IIT Madras.

21	**बोलियों का मूल्यांकन / Evaluation of Bids:** Bid Evaluation will take place in two stages. **Technical Bid evaluation** 1. In the Stage I Bidder will be evaluated first for conformity with bidder Eligibility Criteria – I &II and those bidders who have complied with Bidder Eligibility Criteria – I &II will be evaluated further for technical specifications. 2. Only those bidders who have fully complied with bidder eligibility Criteria – I&II and technical specification will be considered for opening of financial bid. **Stage II: Financial Bid Evaluation** The Lowest financial bid among those who have qualified in the technical bid will be declared as successful bidder (L1) and order will be awarded to the successful bidder (L1).
23	**सफल बोलीदाता का चयन और आदेश प्रदान करना / Selection of successful bidder and Award of Order:** The order will be directly awarded to the technically qualified bidder as per the condition in para 3A of DIPP, MoCI Order No. 45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein.
24	The bidders will not be entertained to participate in opening of Bids. Since the tender is e-tender, the opening of the bids may be checked using the respective logins of the bidders.
25	The pre-bid meetings will be conducted through online. Bidders can submit their queries and doubts to the email id: adstores@iitm.ac.in till the date of the online pre-bid meeting: 25.01.2024 @ 3.30 p.m clarification to the queries and doubts raised by the bidders will be issued as a corrigendum/addendum in the e-tenders portal and Institute Website (tenders.iitm.ac.in). For the bidders, submitting bids on downloaded tender document, it is 'bidders' responsibility to check for any amendment/corrigendum on the website of IIT Madras or check for the same CPP Portal before submitting their duly completed bids. **After the pre-bid meeting, queries/clarification if any will not be considered.**

Sd/-
Assistant Registrar
Stores & Purchase

ACKNOWLEGEMENT

It is hereby acknowledged that I/We have gone through all the points listed under **"Specification and Terms and Conditions"** of tender document, the same is abided and agreed to be executed. In case, if any of the information furnished by me/us is found false, I/We are fully aware that the tender /contract will be rejected / cancelled by IIT Madras and EMD shall be forfeited.

Signature of the Bidder Name & Address of the Bidder with Office Stamp

SCHEDULE OF TENDER

WEB APPLICATION FIREWALL at IIT Madras

Tender No. IITM/SPS/Web Application Firewall/023/2023-24/SPL

Name of Organization	Indian Institute of Technology Madras
Tender Type (Open/Limited/EOI/Auction/Single)	OPEN
Tender Category (Services/Goods/Works)	Goods
Type/Form of Contract (Work/Supply/Auction/ Service/ Buy/ Empanelment/ Sell)	Supply
Name of the Supply	Web Application Firewall at IIT Madras
Source of Fund (Institute/Project)	IIT Madras
Is Multi Currency Allowed	No
Date of Issue/Publishing	22.01.2024
Document Download Start Date	22.01.2024
Document Download End Date	12.02.2024
Prebid Meeting via Google Meet	29.01.2024 @ 03.30 p.m.
Bid Submission Start Date	05.02.2024
Last Date and Time for Uploading of Bids	12.02.2024 @ 02.00 p.m.
Date and Time of Tender Opening	13.02.2024 @ 03.00 p.m.
No. of Covers (1/2/3/4)	2
Bid Validity days (180/120/90/60/30)	120 Days
Address for Communication	**For Technical Queries:** Mr.Anandkumar Computer Center IIT Madras Chennai - 600 036. Phone No: 044- 2257-4987 Email: sanand@zmail.iitm.ac.in **For General Queries:** The Assistant Registrar Stores & Purchase Section IIT Madras Chennai – 600 036 Number 044-2257 8287, Email: adstores@iitm.ac.in.
Contact No.	For Queries : 044- 2257 8287/8288

ANNEXURE – A

Tender No. IITM/SPS/Web Application Firewall/023/2023-24/SPL

Web Application Firewall at IIT Madras

1. BIDDER ELIGIBILITY CRITERIA - I

1) The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**

2) Only 'Class-I local suppliers' and 'Class-II local suppliers', as defined under DIPP, MoCI Order No. P-45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein, shall be eligible to bid in this tender. Declaration for Class-I / Class-II local suppliers should be submitted in the prescribed proforma format as per **Annexure – E.**

2. BIDDER ELIGIBILTY CRIERIA - II

1. Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is **pending** against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure – F.**

2. The firm must have an aggregate financial turnover of at least Rs.28 lakhs in the last 3 years i.e. 2019-20,2020-21 and 2021-22 (Should enclose the audited financial statement signed by the Chartered Accountant)

3. The firm should have an experience of supplying, installing, configuring, implementing and maintaining more than 200 websites out of which at least one should be in educational or Research Institute in India in the past 2 years.

Copies of the document listed below should be submitted as a proof for the above work experience:

a. Work Order
b. User performance Certificate from End User certifying that the firm maintains 200 websites is mandatory.

4. The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-G.**

5. The bidder should have a service centre in Chennai for service support. Proof of Office in Chennai should be furnished as documentary evidence (such as valid rental agreement / registration certificate / Certificate of Incorporation etc.)

3. TECHNICAL SPECIFICATION:

Web Application Firewall – Quantity: 1 No.

S.No	Technical Specification
1	System should support minimum 1 Gbps L7 throughput
2	Proposed solution should have the support for ICSA Lab Certified WAF from day 1 on same appliance
3	Proposed Solution should be IPv6 ready as on day 1
4	The solution should be a hardware based appliance
5	The solution hardware appliance should have minimum 4x1G, 2X10G RJ45 Ethernet ports
6	The solution should support minimum 30,000 ssl transaction per second
7	The solution should support minimum 90,000 HTTP Transactions per second
8	The solution must able to integrate with a Network HSM for crypto processing and storing of PKI information.
9	Solution must offer a “only (detection)” mode that applies the security policies exactly as if it were in prevention mode. The mode setting should be specifiable on a granular level to application security constructs like URL, query/FORM parameters, cookies and header related security rules on an individual basis.
10	The solution must support the following blocking capabilities – connection reset, send custom error response page, redirect the request or block the offending client IP(s) for a time period.
11	The solution must provide HTML rewriting functionality. It should be possible to add, delete and edit request and response headers, translate URL spaces, rewrite or redirect the URL in the request, and rewrite the response body. Regular expression like syntax should be available for the required text manipulations.
12	The Solution should allow the administrator to restrict access to various HTTP and WEBDAV methods including HEAD, CONNECT, TRACE, etc. on a per URL basis.
13	The solution should allow enforcing the following protocol related restrictions on the requests and these should be specifiable on an individual URL basis: a. HTTP method length b. Request line length c. URI length d. Query string length e. Protocol length f. Header name, value, and number g. Request body length h. Cookie name, value and number. i. Parameter name, value and number j. Max length (per file) and number for uploaded files (via POST)

14	The solution should support a positive security model that allows specification of legal "whitelisted" values in various security policy elements, while all other values are denied. E.g.: a. List of allowed values for FORM/query parameters (allowed data types, list, etc) b. List of Allowed meta characters/keywords in URL, parameters c. Valid application profile –– allowed URLs, and the parameters for each URL with individual security profiles for both d. Allowed HTTP methods for each URL e. Allowed Content Types per URL f. File Upload Extensions allowed
15	The solution should provide robust Bot Mitigation and Web Scraping protection capabilities as an integrated feature
16	The solution should provide Application DDOS protection as an inbuilt functionality
17	The solution should provide Volumetric DDOS protection for web assets of a network
18	The solution should provide advanced Malware Inspection capabilities
19	The solution should have the ability to mark fields as read-only to protect against form tampering.
20	The solution should include protection for the common attacks mentioned in the OWASP top ten e.g. SQL Injection, Cross Site Scripting, CSRF, Insecure Direct Object Reference, etc.
21	The product should be able to analyze and secure traffic where a parameter is split across multiple instances.
22	The solution must provide for rate based attack protection a. Protection from Brute Force attacks against access controls. b. Detect brute force attacks (repeated requests for the same resource) against any part of the application. c. React by either slowing or blocking the attacker down. d. Detect brute force attacks against session management (too many sessions given out to a single IP address or range).
23	The Solution should be able protection upload upload protection against zero day malware
24	The solution should protect session tokens, i.e. cookies: a. Sign cookies, to prevent clients from changing them b. Encrypt cookies, to hide contents. c. Prevent Cookie Replay attacks d. Allow for exempting certain cookies from security checks
25	The product should come with a signature database and it should be possible for the WAF to automatically retrieve the latest signatures for the rule database periodically, without manual intervention.
26	The solution should provide comprehensive logging of web attacks, access traffic and admin audit trails.
27	Commonly-used log formats should be supported e.g. Common, W3C extended, NCSA extended etc.
28	Logs should be exportable via syslog and FTP

29	Log information should include session and login identifiers.
30	It should be possible to suppress/mask sensitive parameters from getting logged
31	The solution must provide an easy way to include legitimate requests originally considered as attacks by the current security policy (false positives). This task shouldn't be harder than clicking on a log entry and pushing changes to the WAF.
32	The solution should provide granularity in the way security can be configured for content routing rules i.e. content route specific security policies
33	The solution should provide canned security policies for specific Application Platforms for example SharePoint, outlook web access, WordPress, Joomla, Drupal, Oracle applications etc.
34	The solution should provide a feature to include a unique log id for each transaction, especially for attack logs.
35	The solution should automatically employ intelligent heuristics to learn false positives from request or response traffic and recommend/effect reduction of false positives by modifying the security policies.
36	The solution must provide the ability to define different policies for different applications and provide canned policies for common applications like Outlook Web Access, SharePoint and Oracle.
37	The management components should include facilities to develop custom signatures that identify specific, unique risks associated with protected applications, preferably assisted through a regex tool.
38	The solution should provide a comprehensive “profile learning” process:
39	Configuration facilities to specify trusted hosts that will let the WAF device learn only legitimate traffic.
40	Ability to protect from common web attacks while generating the profile during the training phase.
41	The profile agent should be able to create very specific exceptions where necessary. Creating an exception for a name parameter to allow a name like “John Mc’Donalds” should not allow all SQL patterns, but only ones related to single quotes.
42	The profiler should learn the valid profiles from requests as well as responses. It should be able to parse the response content containing FORM elements to set up parameter profiles from the HTML like max lengths, parameter types – text input, hidden select/dropdowns menus with allowed lists of values on a session as well as global basis.

43	There should be a provision to specify dynamic query parameters for determining unique page profiles. For example, query parameters like “page” and “action”, different values of which will generate different pages with different FORMs etc, even though the URL may remain same (/abc.html?page=1 versus /abc.html?page=2). The profiler should correctly learn these as 2 different URL profiles and not one URL profile for /abc.html with the combined FORMs from both pages.
44	The solution should be configurable end to end using a JSON based REST API framework that can also be extended to support popular configuration management tools like Chef, Puppet and Ansible.
45	The solution should support built in Role Based Access Control for management access
46	The solution should support built in support for authentication users for Role Based Access Control with External Authentication systems using LDAP and RADIUS
47	The solution should support Dual Factor Authentication for management access
48	The solution should support configuration granularity for read/write permissions while created administrator roles
49	The solution should support log analysis using Syslog Integration with popular SIEM solutions such as Splunk, HP Arcsight, Symantec envision etc.
50	The solution should support Network virtualization to support complex traffic routing capabilities and logical network separation of virtual services
51	The solution should support Link Bonding for traffic aggregation
52	The solution should support Link Failover and Redundancy
53	The solution should enable GDPR Compliance
54	The solution should support editable response pages
55	The solution should support Centralized Management using a dedicated centralized management server or using a cloud service
56	The solution should support configuration templates for exporting/importing configuration snippets.
57	The solution should be able to offload user authentication from backend applications. It should be possible to specify custom login and logout pages for user authentication.
58	The authentication module should be able to integrate with external authentication directories such as LDAP, Radius etc.
59	The solution should be able provide for two factor authentication mechanisms, e.g. using client SSL certificates and passwords or by integrating with RSA “SecurID”.

60	It should be possible to specify different authorization policies for different parts of the web sites, post authentication.
61	The solution should allow for single sign on across different protected web applications. The user once authenticated should be able to browse through different applications across single and multiple cookie domains without having to re-login.
62	It should be possible to track full user sessions (complete request and response bodies) and activity by a user id for auditing/troubleshooting purposes as required.
63	The solution should support authenticating user traffic using authentication mechanisms supporting SAML
64	The solution should support Single Sign on and Single Logout functionality for SAML authentication
65	The solution should support authenticating user traffic using ADFS identity and access management
66	The solution should support authenticating user traffic using OKTA identity management

ANNEXURE – B

PROFORMA FOR TECHNICAL COMPLIANCE SHEET

Tender No. IITM/SPS/Web Application/023/2023-24/SPL
Web Application Firewall at IIT Madras

1. BIDDER ELIGIBILITY CRITERIA -I

S. No.		Compliance (Yes / No)	Reference Page No.
1	The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per orders of DIPP OM No. F. No. 6/18/2019-PPD dated 23rd July 2020, and MoCI Order No. P-45021/112/2020-PP (BE II) (E-43780) dated 24th August 2020. A declaration shall be submitted with the bid as per format given in **Annexure – D.**		
2	Only 'Class-I local suppliers' and 'Class-II local suppliers', as defined under DIPP, MoCI Order No. P-45021/2/2017-PP (BE II) dated 16th September 2020 and other subsequent orders issued therein, shall be eligible to bid in this tender. Declaration for Class-I / Class-II local suppliers should be submitted in the prescribed proforma format as per **Annexure – E.**		

2. BIDDER ELIGIBILITY CRITERIA - II

S. No.		Compliance (Yes / No)	Reference Page No.
1	Neither the tender participating firm nor any of its partner has been blacklisted / debarred /involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is **pending** against firm or any partner of the Firm before any Court of Law / Police. A self-declaration format given in **Annexure – F.**		
2	The firm must have an aggregate financial turnover of at least Rs.28 lakhs in the last 3 years i.e. 2019-20,2020-21 and 2021-22 (Should enclose the audited financial statement signed by the Chartered Accountant)		
3	The firm should have an experience of supplying, installing, configuring, implementing and maintaining more than 200 websites out of which at least one should be in educational or Research Institute in India in the past 2 years. **Copies of the document listed below should be submitted as a proof for the above work experience:** a. Work Order **b.** User performance Certificate from End User certifying that the firm maintains 200 websites is mandatory.		
4.	The bidders should be an Original Equipment Manufacturer (OEM) or authorized supplier of OEM. Necessary OEM certificate/OEM authorization letter for this particular tender should be submitted by the bidder as given in **Annexure-G.**		
5.	The bidder should have a service centre in Chennai for service support. Proof of Office in Chennai should be furnished as documentary evidence (such as valid rental agreement / registration certificate / Certificate of Incorporation etc.)		

3. TECHNICAL SPECIFICATION

S. No	Technical Specification	Compliance (Yes/No)	Ref Page no.
1.	System should support minimum 1 Gbps L7 throughput		
2.	Proposed solution should have the support for ICSA Lab Certified WAF from day 1 on same appliance		
3.	Proposed Solution should be IPv6 ready as on day 1		
4.	The solution should be a hardware based appliance		
5.	The solution hardware appliance should have minimum 4x1G, 2X10G RJ45 Ethernet ports		
6.	The solution should support minimum 30,000 ssl transaction per second		
7.	The solution should support minimum 90,000 HTTP Transactions per second		
8.	The solution must able to integrate with a Network HSM for crypto processing and storing of PKI information.		
9.	Solution must offer a “only (detection)” mode that applies the security policies exactly as if it were in prevention mode. The mode setting should be specifiable on a granular level to application security constructs like URL, query/FORM parameters, cookies and header related security rules on an individual basis.		
10.	The solution must support the following blocking capabilities – connection reset, send custom error response page, redirect the request or block the offending client IP(s) for a time period.		
11.	The solution must provide HTML rewriting functionality. It should be possible to add, delete and edit request and response headers, translate URL spaces, rewrite or redirect the URL in the request, and rewrite the response body. Regular expression like syntax should be available for the required text manipulations.		
12.	The Solution should allow the administrator to restrict access to various HTTP and WEBDAV methods including HEAD, CONNECT, TRACE, etc. on a per URL basis.		
13.	The solution should allow enforcing the following protocol related restrictions on the requests and these should be specifiable on an individual URL basis: a. HTTP method length b. Request line length c. URI length d. Query string length e. Protocol length f. Header name, value, and number g. Request body length h. Cookie name, value and number. i. Parameter name, value and number j. Max length (per file) and number for uploaded files (via POST)		

S. No	Technical Specification	Compliance (Yes/No)	Ref Page no.
14.	The solution should support a positive security model that allows specification of legal "whitelisted" values in various security policy elements, while all other values are denied. E.g.: a. List of allowed values for FORM/query parameters (allowed data types, list, etc) b. List of Allowed meta characters/keywords in URL, parameters c. Valid application profile — allowed URLs, and the parameters for each URL with individual security profiles for both d. Allowed HTTP methods for each URL e. Allowed Content Types per URL f. File Upload Extensions allowed		
15.	The solution should provide robust Bot Mitigation and Web Scraping protection capabilities as an integrated feature		
16.	The solution should provide Application DDOS protection as an inbuilt functionality		
17.	The solution should provide Volumetric DDOS protection for web assets of a network		
18.	The solution should provide advanced Malware Inspection capabilities		
19.	The solution should have the ability to mark fields as read-only to protect against form tampering.		
20.	The solution should include protection for the common attacks mentioned in the OWASP top ten e.g. SQL Injection, Cross Site Scripting, CSRF, Insecure Direct Object Reference, etc.		
21.	The product should be able to analyze and secure traffic where a parameter is split across multiple instances.		
22.	The solution must provide for rate based attack protection a. Protection from Brute Force attacks against access controls. b. Detect brute force attacks (repeated requests for the same resource) against any part of the application. c. React by either slowing or blocking the attacker down. d. Detect brute force attacks against session management (too many sessions given out to a single IP address or range).		
23.	The Solution should be able protection upload upload protection against zero day malware		
24.	The solution should protect session tokens, i.e. cookies: a. Sign cookies, to prevent clients from changing them b. Encrypt cookies, to hide contents. c. Prevent Cookie Replay attacks d. Allow for exempting certain cookies from security checks		
25.	The product should come with a signature database and it should be possible for the WAF to automatically retrieve the latest signatures for the rule database periodically, without manual intervention.		
26.	The solution should provide comprehensive logging of web attacks, access traffic and admin audit trails.		

S. No	Technical Specification	Compliance (Yes/No)	Ref Page no.
27.	Commonly-used log formats should be supported e.g. Common, W3C extended, NCSA extended etc.		
28.	Logs should be exportable via syslog and FTP		
29.	Log information should include session and login identifiers.		
30.	It should be possible to suppress/mask sensitive parameters from getting logged		
31.	The solution must provide an easy way to include legitimate requests originally considered as attacks by the current security policy (false positives). This task shouldn't be harder than clicking on a log entry and pushing changes to the WAF.		
32.	The solution should provide granularity in the way security can be configured for content routing rules i.e. content route specific security policies		
33.	The solution should provide canned security policies for specific Application Platforms for example SharePoint, outlook web access, WordPress, Joomla, Drupal, Oracle applications etc.		
34.	The solution should provide a feature to include a unique log id for each transaction, especially for attack logs.		
35.	The solution should automatically employ intelligent heuristics to learn false positives from request or response traffic and recommend/effect reduction of false positives by modifying the security policies.		
36.	The solution must provide the ability to define different policies for different applications and provide canned policies for common applications like Outlook Web Access, SharePoint and Oracle.		
37.	The management components should include facilities to develop custom signatures that identify specific, unique risks associated with protected applications, preferably assisted through a regex tool.		
38.	The solution should provide a comprehensive “profile learning” process:		
39.	Configuration facilities to specify trusted hosts that will let the WAF device learn only legitimate traffic.		
40.	Ability to protect from common web attacks while generating the profile during the training phase.		
41.	The profile agent should be able to create very specific exceptions where necessary. Creating an exception for a name parameter to allow a name like “John Mc’Donalds” should not allow all SQL patterns, but only ones related to single quotes.		

S. No	Technical Specification	Compliance (Yes/No)	Ref Page no.
42.	The profiler should learn the valid profiles from requests as well as responses. It should be able to parse the response content containing FORM elements to set up parameter profiles from the HTML like max lengths, parameter types – text input, hidden select/dropdowns menus with allowed lists of values on a session as well as global basis.		
43.	There should be a provision to specify dynamic query parameters for determining unique page profiles. For example, query parameters like “page” and “action”, different values of which will generate different pages with different FORMs etc, even though the URL may remain same (/abc.html?page=1 versus /abc.html?page=2). The profiler should correctly learn these as 2 different URL profiles and not one URL profile for /abc.html with the combined FORMs from both pages.		
44.	The solution should be configurable end to end using a JSON based REST API framework that can also be extended to support popular configuration management tools like Chef, Puppet and Ansible.		
45.	The solution should support built in Role Based Access Control for management access		
46.	The solution should support built in support for authentication users for Role Based Access Control with External Authentication systems using LDAP and RADIUS		
47.	The solution should support Dual Factor Authentication for management access		
48.	The solution should support configuration granularity for read/write permissions while created administrator roles		
49.	The solution should support log analysis using Syslog Integration with popular SIEM solutions such as Splunk, HP Arcsight, Symantec envision etc.		
50.	The solution should support Network virtualization to support complex traffic routing capabilities and logical network separation of virtual services		
51.	The solution should support Link Bonding for traffic aggregation		
52.	The solution should support Link Failover and Redundancy		
53.	The solution should enable GDPR Compliance		
54.	The solution should support editable response pages		
55.	The solution should support Centralized Management using a dedicated centralized management server or using a cloud Service		
56.	The solution should support configuration templates for exporting/importing configuration snippets.		

S. No	Technical Specification	Compliance (Yes/No)	Ref Page no.
57.	The solution should be able to offload user authentication from backend applications. It should be possible to specify custom login and logout pages for user authentication.		
58.	The authentication module should be able to integrate with external authentication directories such as LDAP, Radius etc.		
59.	The solution should be able provide for two factor authentication mechanisms, e.g. using client SSL certificates and passwords or by integrating with RSA “SecurID”.		
60.	It should be possible to specify different authorization policies for different parts of the web sites, post authentication.		
61.	The solution should allow for single sign on across different protected web applications. The user once authenticated should be able to browse through different applications across single and multiple cookie domains without having to re-login.		
62.	It should be possible to track full user sessions (complete request and response bodies) and activity by a user id for auditing/troubleshooting purposes as required.		
63.	The solution should support authenticating user traffic using authentication mechanisms supporting SAML		
64.	The solution should support Single Sign on and Single Logout functionality for SAML authentication		
65.	The solution should support authenticating user traffic using ADFS identity and access management		
66.	The solution should support authenticating user traffic using OKTA identity management		

**** Reference page number is mandatory and should be mentioned in the technical compliance***

SIGNATURE OF TENDERER ALONG WITH SEAL OF THE COMPANY WITH DATE

ANNEXURE – C

PROFORMA FOR FINANCIAL BID (BoQ)

Tender No. IITM/SPS/ Web Application Firewall /023/2023-24/SPL

WEB APPLICATION FIREWALL at IIT Madras

Sl.No.	Item Description	Qty	Rate per Unit	Total cost(with out GST)	GST (in %)	Total value incl. of GST
1	**Web Application Firewall as per technical specification in Annexure-A**	1			**ENTER AND SUBMIT THE FINANCIAL BID IN THE CPP(e-PROCURMENT PORTAL)**	

NOTE:

- The rate should be inclusive of transporting, loading and unloading.

Place:
Date:

SIGNATURE OF TENDERER ALONG WIT
SEAL OF THE COMPANY WITH DATE

ANNEXURE D

(To be given on the letter head of the bidder)

Tender No. IITM/SPS/ Web Application Firewall /023/2023-24/SPL

Dated: _____

CERTIFICATE

(Bidders from India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I am not from such a country.

OR

(Bidders from Country which shares a land border with India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I am from _____ (Name of Country) and have registered with the Competent Authority. I also certify that I fulfil all the requirements in this regard and am eligible to be considered. *(Copy/ evidence of valid registration by the Competent Authority is to be attached)*

Place:
Date:

Signature of the Bidder
Name & Address of the Bidder with Office Stamp

ANNEXURE – E

FORMAT FOR AFFIDAVIT OF SELF-CERTIFICATION UNDER PUBLIC PROCUREMENT POLICY (PREFERENCE TO MAKE IN INDIA) 2017

Tender No. IITM/SPS/ Web Application Firewall /023/2023-24/SPL

Name of the item / Service: **Web Application Firewall at IIT Madras**

Date: _____

I/We _____S/o, D/o, W/o, _____
Resident of _____
Hereby solemnly affirm and declare as under:

That I will agree to abide by the terms and conditions of the Public Procurement (Preference to Make in India) Policy vide GoI Order no. P-45021/2/2017-PP (B.E.-II) dated 15.06.2017 (subsequently revised vide orders dated 28.05.2018, 29.05.2019and 04.06.2020) MOCI order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P-45021/102/2019-BE-II-Part (1) (E-50310) Dt.4th March 2021 and any subsequent modifications/Amendments, if any and

That the local content for all inputs which constitute the said item/service/work has been verified by me and I am responsible for the correctness of the claims made therein.

Tick (✓) and Fill the Appropriate Category	
☐	I/We_____[name of the supplier] hereby confirm in respect of quoted items thatLocal Content is equal to or more than 50% and come under **"Class-I Local Supplier"** category.
☐	I/We_____[name of the supplier] hereby confirm in respect of quoted items that Local Content is equal to or more than 20% but less than 50% and come under **"Class-II Local Supplier"** category.

The details of the location (s) at which the local value addition is made and the proportionate value of local content in percentage

Percentage of Local content : _____ %**

Location at which value addition done : _____

_____

_____

For and on behalf of..... (Name of firm/entity)

Authorized signatory (To be duly authorized by the Board of Directors)
<Insert Name, Designation and Contact No.>

[Note: In case of procurement for a value in excess of Rs. 10 Crores, the bidders shall provide this certificate from statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.]

This letter should be on the letterhead of the quoting firm and should be signed by a competent authority.

** *Services such as transportation, insurance, installation, commissioning, and training and after sales service support like AMC/CMC cannot be claimed as local value addition*

ANNEXURE - F

(To be given on the letter head of the bidder)

Self-Declaration that the Service Provider has not been Black listed

I …… S/o ……

R/o …… police station …… District …… …….. Director

/ Partner/ sole proprietor (Strike out whichever is not applicable) of ……

…….. (Firm or Company) do hereby declare and solemnly affirm:

I. That the Firm …… ……. has not been Blacklisted or declared insolvent by any of the Union or State Government / Organization.
II. That none of the individual / firm / Company Blacklisted or any partners or shareholder thereof has any connection directly or indirectly with or has any subsistence interest in the deponent business / firm company.
III. That neither the Firm nor any of its partner has been involved / convicted in any criminal case / economic offence nor any criminal case / economic offence is pending against firm or any partner of the Firm before any Court of Law / Police.

Place:
Date:

Signature of the Tenderer
Name & Address of the Tenderer with Office Stamp

ANNEXURE -G

OEM CERTIFICATION FORM

(in Original Letter Head of OEM)

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

We are Original Equipment Manufacturers (OEM) of..... (Name of the company)

Ms..... (Name of the vendor) is one of our Distributors/Dealers/Resellers/Partners (tick one) for the ……. and is participating in the above mentioned tender by offering our product model.....(Name of the product with model number).

…….. is authorized to bid, sell and provide service support warranty for our product as mentioned above.

Name and Signature of the authorized

signatory of OEM along with

seal of the company with Date