भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Request for proposal for procurement of Web Application Firewall Solution

RFP Reference No: NPCI/RFP/2021-22/IT/12 dated 17.11.2021

National Payments Corporation of India
Unit no. 202, 2nd floor,
Raheja Titanium, CTS No. 201,
Western Express Highway,
Goregaon East, Mumbai 400 063
Email- itprocurement@npci.org.in
Website: www.npci.org.in

Copyright Notice

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Bidder or applicants whether verbally or in documentary form by or on behalf of National Payments Corporation of India (NPCI), is provided to the Bidder on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by NPCI to any parties other than the Bidders/ applicants who are qualified to submit the Bids ("Bidders"). The purpose of this RFP document is to provide Bidder with information to assist the formulation of their Proposals. This RFP document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP document and where necessary obtain independent advice. NPCI makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP document. NPCI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

Checklist

The following items must be checked before the Bid is submitted:

1. Online transfer of Rs 11,800/- (Rs. Eleven thousand eight hundred only inclusive of GST@18%) towards cost of Bid document in Envelope/Folder/Folder – 'A'
2. Online transfer / Bank Guarantee of Rs. 5,00,000/- (Rupee Five lakhs only) towards Bid Security in Folder 'A'- Earnest Money Deposit (EMD)

   On account of the COVID-19 pandemic conditions, the bidders shall pay the Bid Cost & EMD through the above mentioned mode and the remittance proof shall be submitted to NPCI for the same, failing which the bid is liable to be rejected.

   Remittance proof in favor of "National Payments Corporation of India" payable at Mumbai" amounting to Rs. 11,800/- (Rs. 10,000/- plus GST @18 %) towards bid purchase cost and Rs. 5,00,000/- towards Bid Security.

   The electronic / wire transfer can be done to designated NPCI bank account as detailed below:
   Account Name: National Payments Corporation of India
   Bank Name: HDFC Bank
   Account No: 00600530001133
   IFSC Code: HDFC0000060
   Address: Maneckji Wadia Bldg., Ground Floor, Naik Motwani Marg, Fort, Mumbai - 400023
   BSR Code: 0510062
   SWIFT Code: HDFCINBBXXX

3. Eligibility Criteria, Technical and Commercial Bids are prepared in accordance with the RFP document.
4. Folder 'A'- Eligibility Criteria Response
5. Folder 'B'- Technical Response
6. RFP document duly sealed and signed by the authorized signatory on each page is enclosed in Folder – 'A'.
7. Prices are quoted in Indian Rupees (INR).
8. All relevant certifications, audit reports, etc. are enclosed to support claims made in the Bid in relevant Envelope/Folder/Folders.
9. All the pages of documents submitted as part of Bid are duly sealed and signed by the authorized signatory.

CHECKLIST **3**

ABBREVIATIONS AND ACRONYMS **7**

SECTION 1 - BID SCHEDULE AND ADDRESS **8**

SECTION 2 – INTRODUCTION **9**

2.1 About NPCI 9
2.2 Objective of this RFP 9
2.3 Cost of the RFP 9
2.4 Due Diligence 9
2.5 Ownership of this RFP 10

SECTION 3 – SCOPE OF WORK **11**

3.1 Scope of work: 11
3.2 Single Point of Contact 11

SECTION 4 – ELIGIBILITY CRITERIA **12**

SECTION 5 - INSTRUCTION TO BIDDERS **15**

5.1 RFP 15
5.2 Cost of Bidding 15
5.3 Content of Bidding Document 15
5.4 Clarifications of Bidding Documents 15
5.5 Amendment of Bidding Documents 15
5.6 Earnest Money Deposit (EMD) 15
5.7 Return of EMD 16
5.8 Forfeiture of EMD 16
5.9 Period of Validity of Bids 16
5.10 Extension of Period of Validity 16
5.11 Format of Bid 16
5.12 Signing of Bid 16
5.13 Envelope/Folder bidding process 16
5.14 Contents of the 3 Envelope/Folder 17
5.15 Bid Submission 17
5.16 Bid Currency 17
5.17 Bid Language 17
5.18 Rejection of Bid 18
5.19 Deadline for Submission 18
5.20 Extension of Deadline for submission of Bid 18
5.21 Late Bid 18
5.22 Modifications and Withdrawal of Bids 18
5.23 Right to Reject, Accept/Cancel the bid 18
5.24 RFP Abandonment 18
5.25 Bid Evaluation Process 18
5.26 Single bid 18
5.27 Price discovery method: 19
5.28 Contacting NPCI 19

SECTION 6 - BID OPENING **20**

6.1 Opening of Bids 20
6.2 Opening of Eligibility and Technical Bids 20

6.3 Opening of Envelope/Folder C - Commercial Bids 20
SECTION 7 - BID EVALUATION 21
7.1 Examination of Eligibility Bids 21
7.2 Examination of Technical Bids 21
7.3 Technical Scoring Matrix: 21
7.4 Evaluation of Commercial Bids: 22
7.5 Successful Evaluated bidder: 22
SECTION 8 - TERMS AND CONDITIONS 23
8.1 Notification of Award / Purchase Order 23
8.2 Term of the Order 23
8.3 Acceptance Procedure 23
8.4 Performance Bank Guarantee 23
8.5 Taxes and Duties 23
8.6 Invoicing Requirements: 24
8.7 Timely Provision of Invoices/ Debit Note/ Credit Note: 24
8.8 Key Deliverables 24
8.9 Delivery schedule 25
8.10 Penalty for default in delivery 25
8.11 End of Sale 25
8.12 Warranties 25
8.13 Support 25
8.14 Service Level Requirements (SLA) 26
8.15 Penalty on non-adherence to SLAs: 28
8.16 Prices 28
8.17 Repeat Order: 28
8.18 Product Upgrades 28
8.19 Payment Terms: 28
8.20 Migration activities for change of location: 29
8.21 Confidentiality 29
8.22 Indemnity 29
8.23 Bidder's Liability 30
8.24 Obligations of the Bidder 30
8.25 Exit option and contract re-negotiation 30
8.26 Extension of Contract 31
8.27 Order Cancellation 31
8.28 Termination of Purchase Order/Contract 31
8.29 Effect of Termination 32
8.30 Force Majeure 32
8.31 Resolution of Disputes 32
8.32 Compliance with Applicable Laws of India 33
8.33 Legal Compliances: 33
8.34 Intellectual Property Rights: 34
8.35 Applicable Law and Jurisdiction 34
8.36 Solicitation of Employees 34
8.37 Facilities provided by NPCI: 34
8.38 No Damage of NPCI Property 34
8.39 Fraudulent and Corrupt Practice 34
8.40 Governing Language 35
8.41 Addresses for Notices 35
SECTION 9 - TECHNICAL SPECIFICATIONS 36

SECTION 10 - DOCUMENTS FORMS TO BE PUT IN FOLDER A 47

ANNEXURE A1 - BIDDER'S LETTER FOR EMD 47

ANNEXURE A2 - BID SECURITY (BANK GUARANTEE) 48

ANNEXURE A3 - BID SECURITY 49

ANNEXURE B - BID OFFER FORM (WITHOUT PRICE) 50

ANNEXURE C - BIDDER INFORMATION 52

ANNEXURE D - DECLARATION FOR CLEAN TRACK RECORD 53

ANNEXURE E - DECLARATION FOR ACCEPTANCE OF RFP TERMS AND CONDITIONS 54

ANNEXURE F - DECLARATION FOR ACCEPTANCE OF SCOPE OF WORK 55

ANNEXURE G - FORMAT POWER OF ATTORNEY 56

ANNEXURE H - ELIGIBILITY CRITERIA COMPLIANCE 57

ANNEXURE I - OEM / MANUFACTURER'S AUTHORIZATION LETTER 62

SECTION 11 - DOCUMENTS TO BE PUT IN ENVELOPE/FOLDER 'B' 63

ANNEXURE J - TECHNICAL COMPLIANCE 63

ANNEXURE K - CLIENT REFERENCE 75

SECTION 12 - DOCUMENTS TO BE PUT IN ENVELOPE/FOLDER 'C' 76

ANNEXURE M - COMMERCIAL BID FORM 76

ANNEXURE N - COMMERCIAL BID 77

ANNEXURE L - BILL OF MATERIAL 78

ANNEXURE Z - NON-DISCLOSURE AGREEMENT 79

Abbreviations and Acronyms

The following abbreviations and acronyms defined in this RFP are as under

BG	Bank Guarantee
DC	Data Centre
EMD	Earnest Money Deposit
IPR	Intellectual Property Rights
LAN	Local Area Network
NPCI	National Payments Corporation of India
OEM	Original Equipment Manufacturer
RFP	Request for Proposal
PBG	Performance Bank Guarantee
SAN	Storage Area Network
SLA	Service Level Agreement
WAN	Wide Area Network
SI	System Integrator
OEM	Original Equipment Manufacturer

Section 1 - Bid Schedule and Address

Sr. No.	Description	
1	Name of Project	Request for proposal for procurement of Web Application Firewall Solution
2	Tender Reference Number	NPCI/RFP/2021-22/IT/12
3	Date of release of RFP	17.11.2021
4	Last date of receiving pre-bid clarifications in writing from vendors	26.11.2021
5	Date and Time for Pre-bid Meeting	Not applicable
6	Last date and time for Bid Submission	10.12.2021 5.30 pm
8	Date and Time of Eligibility & Technical bid Opening	Electronic bid response submission is acceptable to the following email address: **Envelope/Folder A (Eligibility) & Envelope/Folder B (Technical):** siddhesh.chalke@npci.org.in benny.joseph@npci.org.in **Envelope/Folder C:** Commercial bid should be password protected. The password to Commercial bid needs to be shared only upon notification of technical qualification.
9	Date and Time of Commercial Bid Opening	Commercial Bid to be submitted in the Password Protected PDF Document along with Technically Bids. The password to be shared only after request from NPCI's designated authority. NPCI reserves the right to discover the lowest price through Reverse auction OR Price discussion mechanism or both if opted by NPCI. NPCI will inform the method of price negotiation to technically qualified bidders.
10	Name and Address for communication	Head - Strategic IT Procurement National Payments Corporation of India, Unit no. 202, 2nd floor, Raheja Titanium, CTS No. 201, Western Express Highway, Goregaon East, Mumbai 400063
11	Bid Related Queries	Sandeep Tiwari | Contact: +91 9999983500 Email id: sandeep.tiwari@npci.org.in Arvind Patil | Contact: +91 8082044772 Email id: arvind.patil@npci.org.in Benny Joseph| Contact: +91 02240508500 Email id: benny.joseph@npci.org.in Siddhesh Chalke | Contact: +91 8657995380 Email id: siddhesh.chalke@npci.org.in
12	Bid cost	Rs. 11,800/- (Rs. 10,000/- plus GST @18 %)
13	Bid Security	Rs. 5,00,000/- (Rupees Five lakhs only)

Section 2 - Introduction

2.1 About NPCI

NPCI is a Company registered under Section 25 of the Companies Act, 1956 (corresponding to Section 8 of The Companies Act, 2013) with its Registered Office in Mumbai, India. NPCI was promoted by 10 (Ten) banks in India under the aegis of the Indian Bank's Association with majority shareholding by Public Sector Banks. Presently, 54 (Fifty-Four) banks are shareholders of NPCI. Out of which 17 (Seventeen) are Public Sector Banks (PSB), 17 (Seventeen) Private Sector Banks, 3 (Three) Foreign Banks, 10 (Ten) Multi State Cooperative Banks and 7 (Seven) Regional Rural Banks.

The vision, mission and values of NPCI are: Vision - To be the best payments network globally, Mission – Touching every Indian with one or other payment services and to make our mission possible, we live and work by six core values: Passion for Excellence, Collaboration, Customer Centricity, Agility, Security and Innovation.

NPCI, during its journey, has made a significant impact on the retail payment systems in the country. Dedicated to the nation by our former President, Shri Pranab Mukherjee, endorsed by the Hon'ble Prime Minister, Shri Narendra Modi and later made the card of choice for the ambitious Pradhan Mantri Jan Dhan Yojana, RuPay is now a known name. RuPay is an indigenously developed Payment System – designed to meet the expectation and needs of the Indian consumer, banks and merchant eco-system. The alliances with international network partners (Discover Financial Services, Japan Credit Bureau and China Union Pay) provides valuable access to global acceptance footprint and offer world class payment solutions to RuPay cardholders.

NPCI aim is to transform India into a 'less-cash' society by touching every Indian with one or other payment services. With each passing year we are moving towards our vision to be the best payments network globally.

2.2 Objective of this RFP

The objective of the RFP is to procure and deploy a new Web Application Firewall Solution as a replacement of existing NPCINET WAF.

2.3 Cost of the RFP

The Bidder shall bear all costs associated with the preparation and submission of its bid and NPCI will, in no case, be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

2.4 Due Diligence

The Bidders are expected to examine all instructions, terms and specifications stated in this RFP. The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. Also the decision of NPCI on rejection of bid shall be final and binding on the bidder and grounds of rejection of Bid should not be questioned after the final declaration of the successful Bidder.

The Bidder is requested to carefully examine the RFP documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, Bidder should seek necessary clarifications by e-mail as mentioned in Section-1. Any query received after the last date for submission of pre-bid queries as given in Section-1 will not be considered.

2.5 Ownership of this RFP

The content of this RFP is a copy right material of National Payments Corporation of India. No part or material of this RFP document should be published in paper or electronic media without prior written permission from NPCI.

Section 3 – Scope of Work

3.1 Scope of work:

The scope of work will broadly include supply, installation and subsequent maintenance and support for the proposed Web Application Firewall (WAF) Solution. NPCI intends to procure following solution and the broad scope of work will include but not limited to the following:

- To install and configure Web Application Firewall solution at NPCI Data Center and DR center as per the proposed Bill of material.
- Propose Web Application Firewall for DC & DR on a Virtualization platform.
- Instances – 04 Nos. as active-active/Active-Passive for two DC's.
- To configure Web Application Firewall solution at Primary DC and Disaster Recovery site.
- Bidder shall also undertake to carry out implementation / operationalization including move, add, and delete changes / customization of such software updates, releases, version upgrades.
- Bidder should update and maintain all supplied equipment to correctly reflect actual state of the setup at any point in time during the warranty period.
- Bidder should ensure availability of on-site resource if required for troubleshooting and resolution of technical issues back-to-back support from OEM.
- Bidder should support the migration of the Web Application firewall policies and features and building new policies required by organization for the proposed solution during the implementation phase.
- The solution quoted by bidder should not be declared as EOL or EOS(End of Support) by the OEM before the last date of submission of RFP. Bidder to provide the details of the EOL or EOS (End of Support) timelines for the proposed components.
- Bidder to factor and propose software based solution as per their architecture which includes associated monitoring and management software(s) and database license if any.
- Bidder should demonstrate compliance to Technical requirements documented in this document for the solution implemented.
- The bidder / OEM shall provide 24*7*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.
- Implementation of the solution and migration of policies from existing solution to be done by Bidder/OEM directly. Resumes of the team members/SME's to be shared as part of RFP response.
- Bidders are expected to provide the onsite support if the technical issues are not remotely resolved by them.
- Prior to configuration and integration, the bidder needs to understand the requirement of NPCI and prepare detailed implementation plan. On approval of the same by NPCI, integration of the Web Application Firewall solution needs to be carried out. Detailed solution architecture, design, traffic flow and policies (existing) should be documented. Deployment of the solution will start only after acceptance by NPCI.
- The Bidder shall develop a Project Management Plan, should be reviewed by OEM. The plan shall also detail all milestones and indicate when the required deliverable will be available to NPCI.
- The progress of the implementation shall be monitored on regular basis and the deviations, exceptions shall be analyzed and corrective actions to be recommended / suggested.
- The first monitoring report would be submitted on completion of 1 month from the date of acceptance of the Web Application Firewall Solution and thereafter every fortnight with suggested/required remediation.
- The Bidder must prepare architecture design, optimize network to increase performance, documentation, project plan, SOP Documents and training document as part of the implementation services.
- Technical Training should be arranged by OEM directly.

Technical specifications as per Annexure J

3.2 Single Point of Contact

The selected Bidder shall appoint a single point of contact, with whom NPCI will deal with, for any activity pertaining to the requirements of this RFP.

Section 4 – Eligibility Criteria

4.1 Eligibility Criteria

The Eligibility Criteria are furnished below:

A] Start-ups:

Sr. No	Eligibility Criteria
1	The bidder should be incorporated or registered in India under Companies Act/Partnership Act / Indian Trust Act (Annual filling with ROC) and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with NPCI.
2	The bidder's annual turnover should be less than Rs. 100 crores as per audited financial statements in each of the financial years from the date of registration/ incorporation subject to compliance to Sr. No. 3
3	The date of incorporation of the bidder should be anywhere between 1 to 10 financial years.
4	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self- declaration along with extract of auditors' report.
5	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad.
6	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.
7	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission in case the bid document is downloaded from the NPCI website.
8	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.
9	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.

B] Other than start-ups:

Sr. No	Eligibility Criteria	MSME	Other than MSME
1	Registration and incorporation	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act at least since **last 3 years**. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for **at least 2 years** as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act **at least since last 5 years**. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for **at least 5 years** as on date of submission of the bid. b. In case the bidder is the result of a demerger or

		for **at least 2 years** as on the date of submission of bid.	hiving off, at least one of the demerged company or resulting company should have been in operation for **at least 5 years** as on the date of submission of bid.
2	Turnover & profitability	The bidder should have reported minimum annual turnover of Rs. 6 crores and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	The bidder should have reported minimum annual turnover of Rs. 15 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.
3	Governance – Statutory obligations	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.
4	Blacklisting	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad

5	Manufacturer authorization (MAF)	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.
6	Bid cost	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission.
7	Bid earnest money (EMD)	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.
8	Bid participation	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.

Section 5 - Instruction to Bidders

5.1 RFP

RFP shall mean Request for Proposal. Bid, Tender and RFP are used to mean the same. The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding document. Submission of a bid not responsive to the Bidding Document in every respect will be at the Bidders risk and may result in the rejection of its bid without any further reference to the bidder.

5.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid, and NPCI will in no case be responsible or liable for those costs.

5.3 Content of Bidding Document

The Bid shall be in 3 separate Folder A, B and C.

5.4 Clarifications of Bidding Documents

A prospective Bidder requiring any clarification of the bidding Documents may notify NPCI in writing through email any time prior to the deadline for receiving such queries as mentioned in Section 1. The **subject of the email** while sending pre-queries should be titled **"Pre-bid queries - RFP for procurement of Web Application Firewall Solution- NPCI/RFP/2021-22/IT/12 dated 17.11.2021"**

Bidders should submit the queries only in the format given below, in an excel sheet:

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)

Replies to all the clarifications, modifications will be received will be uploaded on NPCI website. Any modification to the bidding documents which may become necessary shall be made by NPCI by issuing an Addendum.

5.5 Amendment of Bidding Documents

1. At any time prior to the deadline for submission of bids, NPCI may for any reason, whether at its own initiative or in response to a clarification requested by a Bidder, amend the Bidding Documents.
2. Amendments will be provided in the form of Addenda to the bidding documents, which will be posted in NPCI's website. Addenda will be binding on Bidders. It will be assumed that the amendments contained in such Addenda had been taken into account by the Bidder in its bid.
3. In order to afford Bidders reasonable time to take the amendment into account in preparing their bids, NPCI may, at its sole and absolute discretion, extend the deadline for the submission of bids, in which case, the extended deadline will be posted on NPCI's website.
4. From the date of issue, the Addenda to the tender shall be deemed to form an integral part of the RFP.

5.6 Earnest Money Deposit (EMD)

The Bidder is required to deposit Rs. 5,00,000/- (Rupees Five lakhs only) in the form of electronic fund transfer/Bank Guarantee in favor of "National Payments Corporation of India" payable at Mumbai or Bank Guarantee issued by a scheduled commercial bank valid for six months, with a claim period of 12 months after the expiry of validity of the Bank Guarantee as per the statutory provisions in this regard, as per format in Annexure A1 or A2. No interest will be paid on the EMD.

The electronic / wire transfer can be done to designated NPCI bank account as detailed below:
Account Name: National Payments Corporation of India
Bank Name: HDFC Bank
Account No: 00600530001133

IFSC Code: HDFC0000060
Address: Maneckji Wadia Bldg., Ground Floor, Naik Motwani Marg, Fort, Mumbai – 400023
BSR Code: 0510062 SWIFT Code: HDFCINBBXXX

5.7 Return of EMD

The EMDs of successful Bidder/s shall be returned / refunded after furnishing Performance Bank Guarantee as required in this RFP. EMDs furnished by all unsuccessful Bidders will be returned on the expiration of the bid validity / finalization of successful Bidder, whichever is earlier.

5.8 Forfeiture of EMD

The EMD made by the bidder will be forfeited if:

1. Bidder withdraws its bid before opening of the bids.
2. Bidder withdraws its bid after opening of the bids but before Notification of Award.
3. Selected Bidder withdraws its bid / Proposal before furnishing Performance Bank Guarantee.
4. Bidder violates any of the provisions of the RFP up to submission of Performance Bank Guarantee.
5. Selected Bidder fails to accept the order within five days from the date of receipt of the order. However, NPCI reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.
6. Bidder fails to submit the Performance Bank Guarantee within stipulated period from the date of acceptance of the Purchase Order. In such instance, NPCI at its discretion may cancel the order placed on the selected Bidder without giving any notice.

5.9 Period of Validity of Bids

Bids shall remain valid for a period of 180 days after the date of bid opening as mentioned in Section 1 or as may be extended from time to time. NPCI reserves the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence.

5.10 Extension of Period of Validity

In exceptional circumstances, prior to expiry of the bid validity period, NPCI may request the Bidders consent to an extension of the validity period. The request and response shall be made in writing. Extension of validity period by the Bidder should be unconditional and irrevocable. The EMD provided shall also be suitably extended. A Bidder may refuse the request without forfeiting the bid Security.

5.11 Format of Bid

The bidder shall prepare one copy (one PDF copy marked as ORIGINAL) of the Eligibility and Technical Bid only. **The commercial bid will be submitted as password protected PDF file.**

5.12 Signing of Bid

The Bid shall be signed by a person or persons duly authorized to sign on behalf of the Bidder. All pages of the bid, except for printed instruction manuals and specification sheets shall be initialed by the person or persons signing the bid.

The bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the Bidder, in which case such corrections shall be initialed by the person or persons signing the Bid.

The bid shall be signed by a person or persons duly authorized to bind the bidder to the contract. Such authority shall be either in the form of a written and duly stamped Power of Attorney (Annexure G) or a Board Resolution duly certified by the Company Secretary, which should accompany the Bid.

5.13 Envelope/Folder bidding process

The Bid shall be prepared in 3 different folders i.e Folder A, Folder B and Folder C.
Each of the 3 folders shall then be sealed and put into an outer Envelope/Folder marked as **"Request for Proposal for procurement of Web Application Firewall Solution".**

In light of the lock imposed due to the COVID-19 pandemic, bids should be submitted through **email.** Folder A (Eligibility) & Folder B (Technical) and Folder C (Commercial) to the following email ids:
siddhesh.chalke@npci.org.in
benny.joseph@npci.org.in

5.14 Contents of the 3 Envelope/Folder

Folder A - Eligibility Bid

The following documents as per the sequence listed shall be inserted inside Folder A:

1 Bid Earnest Money in the form of RTGS **OR** Bid Earnest Money in the form of Bank Guarantee – format provided in **Annexure A2**
2 Bid Offer form (without price) – **Annexure B**
3 Bidder Information – **Annexure C**
4 Declaration of Clean Track Record by Bidder – **Annexure D**
5 Declaration of Acceptance of Terms and Conditions – **Annexure E**
6 Declaration of Acceptance of Scope of Work – **Annexure F**
7 Power of Attorney for signing of bid – **Annexure G**
8 Eligibility Criteria Matrix – **Annexure H**
9 OEM/Manufacturer Authorization Letter – **Annexure I**
10 Audited Balance Sheet and Profit and Loss Statements, Auditors Reports & Notes to accounts for last 3 years
11 CA Certificate that the total turnover has never crossed Rs. 100 Cr since incorporation / registration (if more than 3 years) (only in case of Start-ups)
12 RFP document duly sealed and signed
13 All necessary supporting documents as per Annexures
14 RFP document duly sealed and signed by the authorized signatory on each page
15 All necessary supporting documents

Envelope/Folder B - Technical Bid

The following documents shall be inserted inside Folder B:

1 Section 11 – Compliance to Technical Requirements duly completed - **Annexure J**
2 Client Details for **Annexure K**
3 Masked Price Bid (**Annexure M & N**)
4 Detailed Bill of Material for Software with line item details, giving quantity and functions - **Masked Annexure L**

Technical Bid Folder shall not include any financial information. If the Technical Bid contains any financial information the entire bid will be rejected.

Folder C - Commercial Bid (should be password encrypted)

1 Commercial Bid Form – **Annexure M**
2 Commercial Bid – **Annexure N**
3 Detailed Bill of Material – **Annexure L**

5.15 Bid Submission

The Bidder should bear all the costs associated with the preparation and submission of their bid and NPCI will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process. Bids sealed in accordance with the instructions to Bidders should be delivered at the address as mentioned in the Section 1.

The offers should be made strictly as per the formats enclosed. No columns of the tender should be left blank. Offers with insufficient/inaccurate information and offers which do not strictly comply with the stipulations given in this RFP, are liable for rejection.

5.16 Bid Currency

All prices shall be expressed in Indian Rupees only.

5.17 Bid Language

The bid shall be in English Language.

5.18 Rejection of Bid

The bid is liable to be rejected if the bid document:

a) Does not bear signature of authorized person.
b) Is received through Fax.
c) Is received after expiry of the due date and time stipulated for Bid submission.
d) Is incomplete / incorrect.
e) Does not include requisite documents.
f) Is Conditional.
g) Does not conform to the terms and conditions stipulated in this Request for Proposal.
h) No bid shall be rejected at the time of bid opening, except for late bids and those that do not conform to bidding terms.

5.19 Deadline for Submission

The last date of submission of bids is given in Section 1. However, the last date of submission may be amended by NPCI and shall be notified through its website.

5.20 Extension of Deadline for submission of Bid

NPCI may, at its discretion, extend this deadline for submission of bids by amending the bidding documents which will be informed through NPCI website, in which case all rights and obligations of NPCI and Bidders will thereafter be subject to the deadline as extended.

5.21 Late Bid

Bids received after the scheduled time will not be accepted by the NPCI under any circumstances. NPCI will not be responsible for any delay due to postal service or any other means.

5.22 Modifications and Withdrawal of Bids

Bids once submitted will be treated, as final and no further correspondence will be entertained on this.

No bid will be modified after the deadline for submission of bids.

5.23 Right to Reject, Accept/Cancel the bid

NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever.

NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. NPCI also reserves the right to re-issue the Tender without the Bidders having the right to object to such re-issue.

5.24 RFP Abandonment

NPCI may at its discretion abandon the process of the selection of bidder at any time before notification of award.

5.25 Bid Evaluation Process

The Bid Evaluation will be carried out in 2 stages:

Stage 1 –Folder 'A' i.e. Eligibility bid and **Folder 'B'** i.e. Technical bid will be evaluated. Only those Bidders who have submitted all the required forms comply with the eligibility and technical criteria will be considered for further evaluation.

Stage 2 –Folder 'C' of those Bidders who qualify the eligibility and technical criteria will be evaluated. NPCI reserves the right to conduct Reverse Auction (RA) or Price discussion mechanism or both to arrive the exact price and successful bidder.

5.26 Single bid

In the event of only one responsive bidder or only one bidder emerging after the evaluation process, NPCI may continue with the RFP process.

5.27 Price discovery method:

Bidder to submit their best price. NPCI reserves right to discover the lowest price through the Reverse Auction and/or may be deliberated through Price Discussion Committee if so opted by NPCI management. If first Reverse Auction does not result successful, NPCI reserves the right to call technical qualified bidders for price discussion and declare the successful bidder through Price discussion method instead of conducting 2nd Reverse Auction. The decision with respect to conduct of 2nd Reverse Auction or otherwise shall be communicated to technically qualified bidders.

5.28 Contacting NPCI

From the time of bid opening to the time of Contract award, if any Bidder wishes to contact NPCI for seeking any clarification in any matter related to the bid, they should do so in writing by seeking such clarification/s from an authorized person. Any attempt to contact NPCI with a view to canvas for a bid or put any pressure on any official of the NPCI may entail disqualification of the concerned Bidder and/or its Bid.

Section 6 - Bid Opening

6.1 Opening of Bids

Bids will be opened in 2 stages:

Stage 1 – In the first stage the Eligibility bid i.e. Folder ‘A’ and Technical Bid i.e. Folder ‘B’ will be opened.
Stage 2 – Commercial bids i.e. Folder ‘C’ will be opened for technically qualified bidders for finalizing the prices through the Reverse Auction or the Price discussion method if so opted by NPCI management.

6.2 Opening of Eligibility and Technical Bids

NPCI will open Eligibility bids (Folder ‘A’) and Technical bid (Folder ‘B’) on the date, time and address mentioned in Section 1 or as amended by NPCI from time to time.

6.3 Opening of Envelope/Folder C - Commercial Bids

Bidder to submit their best price. Commercial bids will be opened for Reverse Auction **or** Price discussion(PDC) method with technically qualified bidders if so opted by NPCI management. In case, Commercial evaluation will be done through Reverse Auction, Business Rules and Terms & Conditions and Procedures of Reverse Auction have been published on NPCI’s website i.e. www.npci.org.in.

Section 7 - Bid Evaluation

7.1 Examination of Eligibility Bids

NPCI will examine the bids to determine whether they are complete; whether the required information have been provided as underlined in the bid document; whether the documents have been properly signed and whether the bids are generally in order. Eligibility and compliance to all the forms and Annexure would be the first level of evaluation. Only those Bids which comply to the eligibility criteria will be taken up for further technical evaluation. NPCI may waive any minor informality, non-conformity or irregularity in a bid that does not constitute a material deviation provided such waiver does not prejudice or affect the relative ranking of any Bidder. If a Bid is not substantially responsive, it will be rejected by NPCI and may not subsequently be made responsive by the Bidder by correction of the nonconformity. NPCI's determination of bid responsiveness will be based on the content of the bid itself. NPCI may interact with the Customer references submitted by Bidder, if required.

7.2 Examination of Technical Bids

The Technical Evaluation will be based on the following broad parameters:

a. Compliance to Technical Specifications as specified in the RFP.

b. NPCI reserves the right to call for presentation and discussions on the approach of execution of project etc., from the short-listed Bidders based on the technical bids submitted by them to make an evaluation. Such presentations and minutes of meetings will become part of the technical bid.

c. Review of written reply, if any, submitted in response to the clarification sought by NPCI, if any.

d. Submission of duly signed compliance statement as stipulated in Annexures. Details / Brochures containing details about the proposed hardware are to be enclosed.

e. To assist in the examination, evaluation and comparison of bids, NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

f. NPCI may interact with the Customer references submitted by bidder, if required.

g. NPCI reserves the right to shortlist bidders based on technical evaluation criteria.

h. Bidder should re-submit 2 detailed Bill of material, BOM (one with commercial to IT procurement team and another without commercial to user team) within 3 days if there are any shortfall in BOM found during technical presentation.

Technical Scoring Matrix:

7.3 Technical Scoring Matrix:

TECHNICAL SCORING MATRIX		
Sr. No.	**Description**	**Score**
Technical Evaluation Part - A		30
1	Technical Requirements compliance	
2	Clarity of requirements specified in RFP	
Part - B Vendor Evaluation Matrix		25
1	Customer BFSI reference in India Please provide at least 5 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	
2	Work experience in past (similar project)	
Proposed Solution Part - C		25
1	Approach /Methodology /Quality of Sample reports and RFP documentation	
2	Comprehensiveness of the documents & Project Management Plan	
3	Clarity thought of delivery	

RFP Presentation Part - D		20
1	RFP presentation	
2	Q and A	
	Total Score of Part - A, B, C and D	100

Scoring Matrix: Bidders scoring a minimum of **75% marks** would be eligible for the commercial bid opening.

Basis technical presentation if there are any changes in the BOM, bidders are expected to share the updated BOM with commercials to IT procurement and BOM without commercials to business user team within 3 days. Bidders who do not share the BOM within 3 days will be disqualified.

In the event of only one responsive bidder or only one bidder emerging after the evaluation process, NPCI may continue with the RFP process.

7.4 Evaluation of Commercial Bids:

NPCI reserves the right to discover the lowest price through the Reverse Auction **OR** Price discussion mechanism or both if so opted by NPCI management. NPCI will inform the method of price negotiation to technically qualified bidders.

If first Reverse Auction does not result successful, NPCI reserves the right to call technical qualified bidders for price discussion and declare the successful bidder through Price discussion method instead of conducting 2nd Reverse Auction. The decision with respect to conduct of 2nd Reverse Auction or otherwise shall be communicated to technically qualified bidders. In case, Commercial evaluation will be done through Reverse Auction, Business Rules and Terms & Conditions and Procedures of Reverse Auction have been published on NPCI's website i.e. **www.npci.org.in**

7.5 Successful Evaluated bidder:

The bidder with lowest commercial bid as per Clause 7.4 will be declared as the successful bidder.

In case such Successful Bidder fails to start performing the work required under the Purchase order/Contract, NPCI reserves the right to cancel the Purchase Order/ Contract and de-bar such bidder from participating in future RFPs/ enquiries, if though fit so to do by NPCI. NPCI decision in this respect shall be final and binding on the bidders.

NPCI reserves the right to place the order with the L2 bidder, in case the L1 bidder refuses to accept the order or otherwise gets disqualified as per the terms of the RFP, provided the L2 bidder matches the price quoted by the L1 bidder. In case the 2nd lowest bidder is unable to match the L1 price, NPCI reserves the right to place order with the shortlisted L3 bidder and so on.

Section 8 - Terms and Conditions

8.1 Notification of Award / Purchase Order

After selection of the L1 bidder, as given in Clause # 7.5, and after obtaining internal approvals and prior to expiration of the period of Bid validity, NPCI will send Notification of Award / Purchase Order to the selected Bidder. Once the selected Bidder accepts the Notification of Award the selected Bidder shall furnish the Performance Bank Guarantee to NPCI.

8.2 Term of the Order

The term of the Notification of Award/Purchase Order shall be for a period of 3 years wherein the price of the deliverables as specified in the RFP would be at a fixed rate.

8.3 Acceptance Procedure

- Within 5 days of receipt of Notification of Award/Purchase Order the successful Bidder shall send the acceptance.
- Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

8.4 Performance Bank Guarantee

The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.

8.5 Taxes and Duties

- All taxes deductible at source, if any, shall be deducted at as per then prevailing rates at the time of release of payments.
- Prices shall be exclusive of all taxes.
- The bidder shall meet the requirements of applicable Goods & Services Tax (GST).
- If the invoice raised in any financial year is not settled on or before 30th September of the next financial year, the bidder would be liable to provide a fresh invoice or will accept payment without reimbursement of the GST portion related to such invoice.
- All taxes, if any, shall be deducted at source as per the prevailing rate at the time of release of payments. In case the successful bidder is eligible for “No deduction” or “Lower rate for deduction” of applicable tax at source than the rate prescribed by the Income Tax Act then, the successful bidder shall submit the necessary certificate issued be competent Income Tax authority valid for the period pertaining to the payment. The successful bidder shall meet the requirements of the extant GST legislations.
- If NPCI requests, the successful bidder shall confirm to NPCI in writing that the GST amount charged in invoice is declared in its GSTR-1 and GSTR-3B and payment of GST and other requisite taxes in relation to the invoice has been made. NPCI, in its sole discretion, may decide in consultation with the successful bidder that the invoice will be paid in two batches (i) Base Amount (ii) Tax Amount. NPCI, in its sole discretion, may decide that tax Amount will be paid only after the successful bidder provides sufficient proof that the GST amount charged in invoice is declared in its GSTR-1 and GSTR-3B and payment of requisite taxes has been made.
- The successful bidder agrees to ensure proper discharge of tax liability within statutory time periods with respect to all payments made or to be made to the successful bidder by NPCI. In the event of failure, non-compliance by the successful bidder with the extant GST legislations/Rules and the terms of this clause (including non-compliance that leads to input tax credit not being available to NPCI), NPCI shall be entitled to not release payment and payment shall be kept on hold till such discrepancy is resolved by the successful bidder. Such holding of payments by NPCI

shall not be a breach of its obligations under this Purchase Order. In case of any disputes due to non-matching of GST credit, same shall be resolved by the successful bidder within 30 days of intimation by NPCI, failing which NPCI shall not remit the invoice amount.

- NPCI reserves the right to impose penalty of such amount as may be determined by it up to the value of GST amount involved and any corresponding damages as it may feel appropriate resulting from the successful bidder's breach of any condition or Rule/Regulation of the extant GST legislations or any other applicable tax laws/regulations.

8.6 Invoicing Requirements:

- Invoice/debit note/credit note needs to be issued within 30 days from the date of provision of Deliverables or completion of Services. Further, the invoices/debit note/credit note must cover all the particulars prescribed under GST Invoice Rules. The Successful bidder agrees to comply with invoicing requirements as per GST Invoice Rules and the terms of this clause (including e-invoicing requirements) and/or any other requirement as may be notified by the tax authorities from time to time.
- The Successful bidder invoices/debit note/credit note should be received by NPCI within 2 weeks from the date of issue of invoice.
- The Successful bidder has the obligation to raise invoices/debit note/credit note basis the correct addresses and registration number of the relevant NPCI branch as listed in the Purchase Order

8.7 Timely Provision of Invoices/ Debit Note/ Credit Note:

All necessary invoices and/or adjustment entries to an invoice (Credit Note, Purchase Returns, and Debit Notes) shall be submitted to NPCI by the Successful bidder before September of the succeeding financial year

8.8 Key Deliverables

(Software /Licenses/Implementation/Documentation/OEM Trainings)

1. Supply, installation, maintenance and post implementation support for the entire WAF solution (Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials.
2. Compliance for Software/Instance supplied by bidder/OEM.

Readiness/Compatibility	Virtualization-Compatible
Server	Should be OS Agnostic
Virtualization Environments	Should support Open source Virtualization Platforms/ environments such as Open stack, LinuxKVM etc.

3. Implementation of the complete solution
4. Integrate WAF with all existing applications, infra tools such as AD, PIM, SIEM, SOAR, etc.
5. Detailed implementation reports, HLD's & LLD's.
6. Detailed SOP's for all standard & advanced WAF procedures including but not limited to Monitoring, Failovers, integrations, addition of new Policies/sites/URL's etc.
7. Extensive WAF OEM Administration & troubleshooting Training for NPCI officials & NPCI's service providers (Detailed technical training before Project Kick off and Post Implementation Training)
8. Once successfully configured and deployed, WAF instance testing is to be done by the bidder and should provide test certificate for load testing, Throughput achievement, QAT (Quality Assurance Testing), Hardening documents for WAF's security, performance, quality and functioning.
9. Post Implementation: OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution.

8.9 Delivery schedule

Delivery, installation & commissioning of the proxy solution should be completed within 16 weeks from the date of receipt of purchase order.

- Delivery of hardware, software, and license should be within 6 weeks.
- Installation & commissioning should be completed in next 10 weeks.
- Installation Certificate for each installation should be signed by NPCI and the bidder

8.10 Penalty for default in delivery

If the successful bidder does not deliver & implement the solution as per the above delivery schedule, or such authorized extension of delivery period as may be permitted in writing by NPCI, NPCI shall impose a penalty as given below:

- ✓ Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5%.
- ✓ In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, NPCI reserves the right to cancel the order without prejudice to other remedies available to NPCI
- ✓ Without any prejudice to NPCI's other rights under the Applicable Law, NPCI may recover the liquidated damages, if any, accruing to NPCI, as above, from any amount payable to the supplier, as per the Agreement.

8.11 End of Sale

The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.

8.12 Warranties

The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.

- ✓ The deliverable(s) should not have been declared End of Sale as on the date of submission of the bid and on the date of delivery.
- ✓ The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 3 years (1-year warranty + 2 years AMC) contract period.
- ✓ If the deliverable(s) is declared End of Life (EOL) or End of Support anytime during the contract period, the successful bidder shall forthwith replace the equipment at no additional cost to NPCI.

8.13 Support

The successful bidder shall provide comprehensive on-site maintenance (AMC) of the solution for a period of 3 years with back to back support with the OEM, including warranty period of 1 year and 2 years support post expiry of the warranty period of 1 year.

- ✓ After expiration of warranty period of One (1) year, NPCI at its discretion may enter into Annual Maintenance Contract at the rate mentioned in Purchase Order for period of 2nd and to 3rd year. All the terms and conditions of the Purchase Order will be applicable during such AMC period.
- ✓ Bidder shall maintain all the spares required for maintenance of equipment supplied to NPCI for the period of three (3) years. In case Bidder is not able to repair the equipment due to unavailability of spares, Bidder shall replace the entire equipment with the latest model available in the market with same functionality.
- ✓ Bidder shall provide and install patches/ updates/ version upgrades of all software provided under this contract at no extra cost to NPCI during Warranty and AMC period.

✓ Bidder guarantees the whole of the Goods against any defects or failure, which arise due to faulty materials, workmanship or design (except materials or design furnished by NPCI).If during the Warranty Period any Goods/software are found to be damaged or defective or not acceptable, they shall promptly be replaced or rectified /re-furnished or rendered by Bidder at its own cost (including the cost of dismantling and reinstallation) on the request of NPCI and if removed from the Site for such purpose, Bidder has to provide standby Goods till the original Goods are repaired or replaced / re-furnished, rendered. All goods shall be removed and redelivered to NPCI by Bidder at its own cost.

8.14 Service Level Requirements (SLA)

The SLA specifies the expected levels of service to be provided by the Bidder to NPCI. This expected level is also called the baseline. Any degradation in the performance of the solution and services is subject to levying penalties.

Payments to the Bidder are linked to the compliance with the SLA metrics. During the contract period, it is envisaged that there could be changes to the SLAs, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. NPCI and Bidder.

The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to NPCI or its designated personnel to the tools used for SLA monitoring.

Definitions

1. "Availability" means the time for which the services and facilities are available for conducting operations on the AIC system including application and associated infrastructure.
   Availability is defined as (%) = $\frac{\text{(Operation Hours –Downtime)}}{\text{(Operation Hours)}}$ * 100%
2. The business hours are 24*7*365 on any calendar day the NPCI is operational.
3. All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.
4. The "Operation Hours" for a given time frame are calculated after deducting the planned downtime from "Operation Hours". The Operation Hours will be taken on 24x7 basis, for the purpose of meeting the Service Level requirements i.e. availability and performance measurements both.
5. "Downtime" is the actual duration for which the system was not able to service NPCI or the Clients of NPCI, due to System or Infrastructure failure as defined by NPCI and agreed by the Bidder.
6. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during business hours. Further, scheduled maintenance time is planned downtime with the prior permission of NPCI.
7. "Incident" refers to any event / abnormalities in the functioning of any of IT Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.

Interpretation & General Instructions

1. Typical Resolution time will be applicable if systems are not available to the NPCI's users.
2. The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. The Bidder is expected to provide the following service levels. In case the service levels defined in the tables below cannot be achieved, it shall result in a breach of contract and invoke the penalty clause.
3. A Service Level violation will occur if the Bidder fails to meet Minimum Service Levels on a monthly basis for a particular Service Level.
4. Quarterly SLAs would be analyzed. However, there would be month wise SLAs and all SLA targets have to be met on a monthly basis.
5. Overall Availability and Performance Measurements will be on a quarterly basis for the purpose of Service Level reporting. Month wise "Availability and Performance Report" will be provided by the

Bidder for every quarter in the NPCI suggested format and a review shall be conducted based on this report. Availability and Performance Report provided to NPCI shall contain the summary of all incidents reported and associated performance measurement for that period.

6. The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for cutting fees.

Severity Levels

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA's will be applicable post go-live of Compliance Solution at DC, DRS and other NPCI Offices.

Description: Time taken to resolve the reported problem Severity is defined as:

Level	Function/Technologies
Severity 1	i Such class of errors will include problems, which prevent users from making operational use of solution. ii Security Incidents iii No work-around or manual process available iv Financial impact on NPCI v Infrastructure related to providing solution to the NPCI users comprising of but not limited to the following: a. Proposed Solution Tools / Application Servers b. Proposed Solution Database Servers / Appliance c. Proposed Solution servers/appliances d. Network components, if any proposed by the bidder
Severity 2	i Any incident which is not classified as "Severity 1" for which an acceptable workaround has been provided by the Bidder or; ii Any problem due to which the Severity 2 infrastructure of the proposed solution is not available to the NPCI users or does not perform according to the defined performance and query processing parameters required as per the RFP or; iii Users face severe functional restrictions in the application irrespective of the cause. iv Key business infrastructure, systems and support services comprising of but not limited to the following: a The Solution Test & Development and Training Infrastructure and Application b Infrastructure for providing access of dashboards, scorecards, etc.
Severity 3	i Any incident which is not classified as "Severity 2" for which an acceptable workaround has been provided by the Bidder; ii Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround. iii No impact on processing of normal business activities iv Equipment/system/Applications issues and has no impact on the normal operations/day-today working. v All other residuary proposed solution Infrastructure not defined in "Severity 1" & "Severity 2"

During the term of the contract, the bidder will maintain the solution in perfect working order and condition and for this purpose will provide the following repairs and maintenance services

8.15 Penalty on non-adherence to SLAs:

The following Resolution Service Level Agreement (SLA) would be applicable during Warranty and AMC and are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only.

a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total AMC value.

b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total AMC value.

c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total AMC value.

d) The penalty amount would be calculated and deducted from the performance bank guarantee during warranty period and from the AMC charges payable during the period of AMC.

e) Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly.

f) If a breach occurs even after a proper policy in Web Application Firewall solution is in place, a penalty of Rs. 10,000/- per event will be deducted or the loss due to the breach whichever is higher. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

8.16 Prices

Price shall remain fixed for a period of 3 years from the date of Notification of award / 1st Purchase Order. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained.

8.17 Repeat Order:

NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and/or services included in the Solution at the agreed unit rate for individual categories of purchase order during the period of 3 years from the date of award / 1st Purchase Order.

8.18 Product Upgrades

Notwithstanding what is contained and provided in Clause # 8.8 herein above, at any time during term of the purchase order / performance of the Contract, should technological advances be introduced by the OEM/ Bidder for information technologies originally offered by the supplier in its bid and still to be delivered, the bidder shall be obliged to offer to NPCI the latest version of the available technologies having equal or better performance or functionality throughout the contract period without any extra cost to NPCI.

During performance of the Contract, the bidder shall offer to NPCI all new versions, releases and updates of standard software, as well as related technical support within 30 days of their availability from the OEM.

8.19 Payment Terms:

- Software/Licenses: Payment shall be released within 30 days after delivery of the software /licenses along submission of correct invoice with necessary supporting documents and delivery report duly signed by NPCI officials
- Installation/Implementation Charges: Payment shall be released within 30 days after successful implementation upon submission of correct invoice along with necessary supporting documents i.e. implementation/installation report duly signed by NPCI officials.
- AMC: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.

- If the invoice raised in any financial year is not settled on or before 30th September of the next financial year, the vendor would be liable to provide a fresh invoice or will accept payment without reimbursement of the GST portion related to such invoice.
- The vendor shall comply with all the applicable Goods & Services Tax (GST) legislations as decided by the Government from time to time.
- Payment will be released within 30 days of receipt of correct invoices along with necessary documents / certificates duly signed by authorized NPCI official.
- For the purpose of payment, the end of the quarter will be June, Sept, Dec and March.
- Invoice shall contain all details regarding PAN & registration number for GST.

8.20 Migration activities for change of location:

In case NPCI wishes to shift the devices/software/service (if any) from one place to another anywhere in the country, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of devices/software/service supplied by Service provider & hand-over to the concerned Officials or Data Center, pre-shifting inspection, post-shifting inspection, re-installation etc. of all devices supplied by Service provider. All migration related activities to be done after Business / session hours /according to business convenience & the engineer has to be deployed as per the requirements. NPCI will bear all expenses for packing, shifting, insurance and other incidentals at actual. NPCI will not be responsible or liable for any losses, damages to the items of equipment's, tools and machinery while such dismantling, pre-shifting inspection, post-shifting inspection, and re-installation etc. is being carried out. Bidder shall make available adequate alternative arrangement to ensure that the system functioning is neither affected nor dislocated during the shifting process. It is the responsibility of field engineer to integrate devices delivered at required location or Data Center & coordinate with NPCI NOC to extend the reachability.

8.21 Confidentiality

The Successful bidder shall treat the details of this PO and other contract documents executed between NPCI and the successful bidder as secret and confidential. The Successful bidder shall execute separate NDA on the lines of the format provided in the Annexure Z hereof.

In the event of disclosure of Confidential Information to a third party in violation of the provisions of this Clause, the Successful bidder shall use all reasonable endeavors to assist NPCI in recovering and preventing such third party from using, selling or otherwise disseminating of such information. The Parties' obligations under this Section shall extend to the non-publicizing of any dispute arising out of PO.

The terms of this clause shall continue in full force and effect for a period of five (5) years from the date of disclosure of such Confidential Information.

In the event of termination of this PO, upon written request of the NPCI, The Successful bidder shall immediately return the Confidential Information of NPCI, or at the NPCI's option destroy any remaining Confidential Information and certify that such destruction has taken place.

8.22 Indemnity

The bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting from any act or omission or negligence or misconduct of the bidder and its employees and representatives, breach of the terms and conditions of the agreement or purchase order, false statement by the bidder, employment claims of employees of the bidder, third party claims arising due to infringement of intellectual property rights, death or personal injury attributable to acts or omission of bidder, violation of statutory and regulatory provisions including labour laws, laws related to information technology and intellectual property rights, breach of confidentiality obligations, breach of warranty, etc.

Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect, consequential and incidental damages and compensation. Bidder shall indemnify NPCI, provided NPCI promptly notifies the Bidder in writing of such claims and the Bidder shall have the right to undertake the sole defense and control of any such claim.

8.23 Bidder's Liability

The selected Bidder will be liable for all the deliverables.
The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order.

The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

8.24 Obligations of the Bidder

Standard of Performance: The Bidder shall perform the services and carry out their obligations with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment materials and methods. The Bidder shall always act in respect of any matter relating to this Contract or to the services as faithful advisor to NPCI and shall at all times support and safeguard NPCI's legitimate interests in any dealings with third parties.
Prohibition of Conflicting Activities: The Bidder shall not engage and shall cause their personnel not to engage in any business or professional activities that would come in conflict with the activities assigned to them under this RFP.

8.25 Exit option and contract re-negotiation

a) NPCI reserves its right to cancel the order in the event of happening of one or more of the situations as mentioned in the "Order Cancellation" herein under.
b) Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder should continue to provide the facilities to NPCI at NPCI's locations.
c) Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the bidders prior to expiry of time for awarding the final bid / the contract. The Bidder should perform a reverse transition mechanism to NPCI or its selected vendor. The reverse transition mechanism would facilitate an orderly transfer of services to NPCI or to an alternative 3rd party / vendor nominated by NPCI. Where NPCI elects to transfer the responsibility for service delivery to a number of vendors, NPCI will nominate a vendor who will be responsible for all dealings with the Bidder regarding the delivery of the reverse transition services.
d) The reverse transition services to be provided by the Bidder shall include the following:
   i. The Bidder shall suitably and adequately train NPCI or its designated team for fully and effectively manning, operating the Devices.
   ii. Bidder shall provide adequate documentation thereof.
   iii. The Bidder shall jointly manage the Devices with NPCI or designated team for a reasonable period of time
e) Knowledge Transfer: The Bidder shall provide such necessary information, documentation to NPCI or its designee, for the effective management and maintenance of the Deliverables under this RFP/Purchase Order/contract. Bidder shall provide documentation (in English) in electronic form where available or otherwise a single hardcopy of all existing procedures, policies and programs required for supporting the Services.
f) Warranties:
   1. All the warranties held by or in the name of the bidder shall be assigned or transferred as-is, in the name of NPCI. The bidder shall execute any and all such documents as may be necessary in this regard.
   2. The bidder shall return confidential information and will sign off and acknowledge the return of such confidential information.
   3. The bidder shall provide all other services as may be agreed by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and priced.

4. The bidder recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the bidder under the scope, upon termination or expiration thereof, for any reason whatsoever.

g) The rates for availing services during reverse transition period would be the same as payable during the contract period for the respective services as contained and provided in this RFP.

h) During which the existing Bidder would transfer all knowledge, know-how and other things necessary for NPCI or new bidder to take over and continue to manage the services. The Bidder agrees that the reverse transition mechanism and support during reverse transition will not be compromised or affected for reasons whatsoever is for cancellation.

i) NPCI shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.

j) NPCI and the successful bidder shall together prepare the Reverse Transition Plan. However, NPCI shall have the sole decision to ascertain whether such Plan has been complied with.

k) The Bidder agrees that in the event of cancellation or exit or expiry of the RFP/Purchase Order/contract it would extend all necessary support to NPCI or its selected vendors as would be required

8.26 Extension of Contract

The bidder shall be required to consistently execute, in a successful and professional manner, the jobs assigned under this RFP or subsequent Purchase Order / Contract, as shall be entered by NPCI with the Bidder, to the satisfaction of and as decided by the NPCI up to a period of three (3) years (completion period) reckoned from the date of commencement of the services and may be extended for further period on satisfactory performance by bidder. However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 6 months' period on the same rates and terms & conditions of the Contract. NPCI has right to alter (increase or decrease) the number of resources. NPCI has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by NPCI.

8.27 Order Cancellation

NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone;

i. Delay in delivery is beyond the specified period as set out in the Purchase Order before acceptance of the product; or,

ii. Serious discrepancy in the quality of service expected.

iii. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the bidder turns out to be incorrect and/or bidder conceals or suppresses material information.

In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the original amount paid.

8.28 Termination of Purchase Order/Contract

For Convenience: NPCI, by written notice sent to Bidder, may terminate the Purchase Order/ contract in whole or in part at any time for its convenience giving three months' prior notice. The notice of termination may specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective. NPCI shall consider request of the bidder for pro-rata payment till the date of termination.

For Insolvency: NPCI at any time may terminate the contract by giving written notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI.

For Non-Performance: NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI).

8.29 Effect of Termination

- The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment.
- Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services
- The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI.
- NPCI shall make such prorated payment for services rendered by the Bidder and accepted by NPCI at the sole discretion of NPCI in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder.
- NPCI may make payments of undisputed amounts to the Bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies NPCI may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.
- Upon cancellation of contract/completion of period of service, the Bidder should peacefully handover the legal possession of all the assets provided and obtains discharge from NPCI. NPCI also reserves the right to assign or allot or award the contract to any third party upon cancellation of the availed services.

8.30 Force Majeure

For purpose of this clause, "Force Majeure" means an unforeseeable event beyond the control of the successful and not involving NPCI or the successful 's fault or negligence.

If either party is prevented, restricted, delayed or interfered by reason of: a) Fire, explosion, cyclone, floods, droughts, earthquakes, epidemics; b) War, revolution, acts of public enemies, blockage or embargo, riots and civil commotion; c) Any law, order, proclamation, ordinance or requirements of any Government or authority or representative of any such Government, including restrictive trade practices or regulations; d) Strikes, shutdowns or labour disputes which are not instigated for the purpose of avoiding obligations herein; or e) Any other circumstances beyond the control of the party affected; then notwithstanding anything here before contained, the party affected shall not be liable for non-performance of delay in performance of its obligations contained herein provided the party so affected uses its best efforts to remove such cause of non-performance, and when such cause is removed the party shall continue performance in accordance with the terms of the Purchase Order.

Each of the parties agrees to give written notice forthwith to the other upon becoming aware of an event of Force Majeure, the said notice to contain details of the circumstances giving rise to the event of Force Majeure. If the event of Force Majeure continues for more than twenty (20) days, either party shall be entitled to terminate the Purchase Order at any time thereafter by giving written notice to the other party

8.31 Resolution of Disputes

All disputes or differences between NPCI and the bidder shall be settled amicably. If, however, the parties are not able to resolve them, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

NPCI and the successful Bidder shall make every effort to resolve amicably by direct informal negotiation; any disagreement or dispute arising between them under or in connection with this RFP.

If, however, NPCI and successful Bidder are not able to resolve them, following dispute resolution mechanism shall be applied:

1. In case of Dispute or difference arising between NPCI and the successful Bidder relating to any matter arising out of or connected with this RFP, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by NPCI and the successful Bidder. The third Arbitrator shall be chosen by mutual discussion between NPCI and the successful Bidder.
2. Arbitration proceedings shall be held at Mumbai, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English;
3. The decision of the majority of Arbitrators shall be final and binding upon NPCI and Successful Bidder. The cost and expenses of Arbitration proceedings will be paid as determined by mutual chosen third Arbitrator. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself; and
4. Where the value of the contract is Rs.1.00 Crore and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by mutual consent between the parties.
5. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

8.32 Compliance with Applicable Laws of India

The Bidder confirms to NPCI that it complies with all Central , State, Municipal laws and local laws and rules and regulations and shall undertake to observe, adhere to, abide by, comply with and notify NPCI about compliance with all laws in force including Information Technology Act 2000, or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and for all purposes of this RFP, and shall indemnify, keep indemnified, hold harmless, defend and protect NPCI and its officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this RFP or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the RFP, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NPCI and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NPCI and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and NPCI will give notice of any such claim or demand of liability within reasonable time to the Bidder.

8.33 Legal Compliances:

The Bidder confirms to NPCI that its personnel/ employees/staff are covered under the provision of various Acts enacted for the protection and benefits of workmen /employees /staff or otherwise such as Employees State Insurance Act and Employees Provident Fund Miscellaneous Provision Act etc. and such other Acts like Profession Tax Act etc. as applicable and that Bidder is duly registered under the provisions of the said Acts and is complying with the provisions of the Acts.

The Bidder shall allow NPCI as well as regulatory authorities to verify books in so far as they relate to compliance with the provisions of these Acts and shall provide on demand by NPCI & regulatory authorities such documentary proof as may be necessary to confirm compliance in this regard. NPCI shall not be responsible in any event to the employees of Bidder for any of their outstanding claims or liability in that regard. NPCI shall not be responsible for any claim or demand made by such personnel for their dues outstanding against Bidder. Bidder indemnifies and shall keep NPCI indemnified from any of such claims/ losses/ damages and demands by any of its personnel, if any, raised on NPCI.

8.34 Intellectual Property Rights:
All rights, title and interest of NPCI in and to the trade names, trademark, service marks, logos, products, copy rights and other intellectual property rights shall remain the exclusive property of NPCI and Bidder shall not be entitled to use the same without the express prior written consent of NPCI. Nothing in this RFP including any discoveries, improvements or inventions made upon with/by the use of the Bidder or its respectively employed resources pursuant to contract shall either vest or shall be construed so that to vest any proprietary rights to the Bidder.
Notwithstanding, anything contained in this RFP, this clause shall survive indefinitely, even after termination of this Purchase Order.

8.35 Applicable Law and Jurisdiction
Applicable Law: The Agreement shall be governed by and interpreted in accordance with the Indian Law. The jurisdiction and venue of any action with respect to the subject-matter of this Agreement shall be the Courts of Mumbai in India and each of the parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such action.

8.36 Solicitation of Employees
Both NPCI & successful Bidder the Parties should agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties should agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge to directly or indirectly solicit of this contract for employing the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

8.37 Facilities provided by NPCI:
NPCI shall provide seats, with required facilities like internet, intranet & LAN Connectivity free of cost for official work. These facilities shall not be used for any personal use. In case of any misuse of the facilities, penalty as deemed fit shall be imposed and recovered from the pending bills of Bidder.

8.38 No Damage of NPCI Property
Bidder shall ensure that there is no loss or damage to the property of NPCI while executing the Contract. In case, it is found that there is any such loss/damage due to direct negligence/non-performance of duty by any personnel, the amount of loss/damage so fixed by NPCI shall be recovered from Bidder.

8.39 Fraudulent and Corrupt Practice
"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of the project and includes collusive practice among Bidder's (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the NPCI of the benefits of free and open competition.

“Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official or a NPCI official in the process of project execution. NPCI will reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing the project.

8.40 Governing Language

All correspondences and other documents pertaining to this Agreement shall be in English only.

8.41 Addresses for Notices

Following shall be address of NPCI and Bidder
NPCI address for notice purpose:
Managing Director& CEO

National Payments Corporation of India
1001A, B wing 10th Floor,
‘The Capital’, Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051
Supplier’s address for notice purpose: (To be filled by supplier)

Section 9 - Technical Specifications

Sr. No.	Specifications for Web Application Firewall	Requirement
1	**General Features & Requirements**	
1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Must Have
1.2	The vendor/bidder must be Gold/Tier-1 or Silver/Tier-2 or Authorized partner of the OEM for the proposed product.	Must Have
1.3	The bidder should have back to back arrangement with the OEM so that NPCI will be able to log a call with the OEM directly.	Must Have
1.4	The bidder should have support offices in Mumbai, Hyderabad and Chennai.	Must Have
1.5	The bidder should have minimum 2 skilled OEM certified staff (Web Application Firewall - Subject Matter Experts) for the product proposed.	Must Have
1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	Must Have
1.7	There must be minimal impact on the existing applications and the network architecture when deploying or removing the solution from the network.	Must Have
1.8	The Proposed Solution should have capability to deploy/integrate in Virtualized Environment/Opensource environments - Openstack, LinuxKVM etc.	Must Have
1.9	The proposed solution should provide integrated functionalities of server load balancer, SSL Offloading, SSL Bridging.	Must Have
1.10	The proposed solution must support TCP multiplexing, TCP optimization and dynamic Service chaining for SSL Offload with TCP session mirroring and persistence mirroring, compression, caching etc. in active-passive mode.	Must Have
1.11	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event	Good to have
1.12	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration	Must Have
1.13	The Proposed Solution should have option be manageable from a single management platform, Single management platform to manage policies across DC & DR.	Good to have
1.14	The proposed solution should have a feature to generate device snapshot reports which then should be uploaded to an OEM provided online tool and get feedback on the health of the unit & missing Hotfixes and best practices	Must Have
1.15	The proposed solution should provide minimum of 3 Gbps WAF Throughput per instance from day one (With all WAF functions enabled per instance in blocking mode) with sub millisecond latency.	Must Have
1.16	The Proposed Solution should have support for multiple VLANs with tagging capability	Must Have
1.17	The Proposed Solution should have capability to support minimum 50000 https Concurrent Connections scalable to 100000 https Concurrent Connections.	Must Have
1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Must Have
1.19	Should support IPv4 & IPv6 addressing, IPv6 client and IPv4 servers with NAT44/NAT66/NAT64/NAT46 with full support for IPv6	Must Have

1.20	Should support routing protocols RIP, OSPF and BGP to participate in Dynamic routing	Good to have
1.21	Should have ability to upgrade/downgrade device software Images.	Must Have
1.22	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.	Must Have
2	**SSL/TLS Handling**	
2.1	The proposed solution should facilitate SSL handling.	Must Have
2.2	The system must be able to establish SSL session before sending any packet to backend servers	Must Have
2.3	The system must support elliptic curve cryptography (ECC)	Must Have
2.4	The system must support SSL/TLS client certificate authentication	Must Have
2.5	The system should support TLS v1.1, v1.2, TLS v1.3, SSL v2 & SSL v3 (Highest version available)	Must Have
2.6	Proposed solution should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for each application service	Must Have
2.7	The system must store the certificate private key using a secure mechanism (With & without passphrase)	Must Have
2.8	The system must capable of communication with the original backend application server / Application service over SSL or TLS. should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL/TLS connection to the backend server	Must Have
2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Must Have
2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	Must Have
3	**Web Application Firewall**	
3.1	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.	Must Have
3.2	Proposed solution should be ICSA Lab Certified WAF	Good to have
3.3	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution).	Must Have
3.4	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions to address the compliances and configure policies for it.	Must Have
3.5	When deployed as a full proxy mode, the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.	Must Have
3.6	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	Must Have
3.7	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over.	Must Have
3.8	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat	Must Have

	Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	
3.9	The solution must be able to validate encoded data in the HTTP traffic	Must Have
3.10	The solution must be able to identify Web Socket connections and provide security for WebSocket including security for exploit against Server abuse, login enforcement, XSS and SQL injection. The Solution must be able to parse and monitor JSON data over web socket protocol	Must Have
3.11	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	Must Have
3.12	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.	Must Have
3.13	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	Must Have
3.14	The Proposed Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions	Must Have
3.15	The Proposed Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.	Must Have
3.16	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.	Must Have
3.17	The Proposed WAF Solution Should support ICAP, API or other supporting integration with different security devices for file scanning, sandboxing requests etc (industry leading security solutions i.e Symantec, McAfee, Trend Micro etc)	Must Have
3.18	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Must Have
3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Must Have
3.20	Proposed Solution should have ability to automatically detect application platform and its technology used on backend side to define signature sets required for defined Proposed Solution policy.	Must Have
3.21	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy	Must Have
3.22	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.	Must Have
3.23	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.	Must Have
3.24	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	Must Have
3.25	Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc.	Must Have
3.26	Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application	Must Have
3.27	Proposed WAF Solution should have capability to learn changes in the already integrated Web Application & protect it at the same time i.e. solution should be able to learn changes in the application in the	Must Have

	Protection Mode. Proposed Solution should have option to learn policy and configure the application in block mode simultaneously	
3.28	The WAF Solution should have ability to configure application in block mode partially and learn the traffic for filters whose fine tuning is yet to be configured	Must Have
3.29	Should be able to uniquely detect and block if required the end user on the basis of internal IP address, Plugins Installed in the browser, OS, Screen Resolution, Fonts etc. instead of going with traditional IP based blocking only	Must Have
3.30	Solution should dynamically understand the Changes on the Web/Application Server	Must Have
3.31	Should provide Policy creation per URL and not generic policy for URL's	Must Have
3.32	System should protects against the following threats/attacks: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Stealth commanding • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping • Directory/Path traversal • Remote File Inclusion	Must Have
3.33	System supports enforcing policies regardless of character encoding in order to combat evasion techniques, WAF should support Policy Evasion Detection Engine to combat evasion techniques such as: • URL-decoding (for example, %XX) • Self-referencing paths (that is,. use of /./ and encoded equivalents) • Path back-references (that is, use of /../ and encoded equivalents) • Mixed case • Excessive use of whitespace • Comment removal (for example, convert DELETE/**/FROM to DELETE FROM) • Conversion of (Windows-supported) backslash characters into forward slash characters. • Conversion of IIS-specific Unicode encoding (%uXXYY) • IIS extended Unicode • Virtual directory route—positive folder enforcement • Base64 Encoded parameters & headers	Must Have
3.34	The solution must provide the following features and protection: a. HTTP protocol validation b. Correlated based attack protection c. HTTP protocol attack signatures d. Cookie signing validation e. Anti-website scraping f. Whitelisting based protection g. Web worm protection h. Web application attack signatures i. Web application layer customized protection	Must Have

3.35	The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP attacks g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. Parser protection (XML Bombs, Recursion Attacks)	Must Have
3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	Must Have
3.37	Should support XML Applications - solution must be able to protect web applications that include Web services (XML) content.	Must Have
3.38	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.	Must Have
3.39	The proposed WAF should support XML islands	Must Have
3.40	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.	Must Have
3.41	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)	Good to have
3.42	The system must capable of blocking specific list of HTTP methods	Must Have
3.43	The system must be able to allow or disallow specific file type	Must Have
3.44	The system must be able to enforce specific HTTP headers and values to be present in client requests	Must Have
3.45	The system must be able to perform information display masking/scrubbing on requests and responses	Must Have
3.46	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user d. Block the IP address	Must Have
3.47	The solution must be able to block the user or the IP address for a configurable period of time	Must Have
3.48	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode	Good to have
3.49	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2.	Must Have
3.50	The solution must be able to decrypt SSL web traffic between clients and web servers	Must Have
3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	Must Have
3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	Must Have

3.53	The solution must include a pre-configured list of comprehensive and accurate web attack signatures	Must Have
3.54	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	Must Have
3.55	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must have an option to be continuously and automatically updated	Must Have
3.56	The solution must support regular expressions for the following purposes: a. Signatures definition b. Sensitive data definition c. Parameter type definition d. Host names and URL prefixes definition e. Fine tuning of parameters that are dynamically learnt from the web application profiles	Must Have
3.57	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic	Must Have
3.58	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP requests and responses, HTTP(S) headers, form fields, and the HTTP(S) body	Must Have
3.59	The solution must be able to inject HTML snippet/text in the HTTP response	Must Have
3.60	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header	Must Have
3.61	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header	Must Have
3.62	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	Must Have
3.63	The solution must be capable to automatically create whitelisting/profiling of web applications.	Must Have
3.64	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria.	Must Have
3.65	The solution must be able to perform virtual patching for its protected web applications.	Must Have
3.66	The solution must support the capability to define security policies based on the threat intelligence feeds listed previously to perform the following functions: a. Alert b. Block IP c. Block Session d. Block User	Must Have
3.67	The proposed Solution should be session aware and should be able to enforce and report session	Must Have
3.68	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.	Good to have
3.69	The proposed Solution should be able to protect against Manipulation of invalidated input	Must Have
3.70	The proposed Solution should protect against requests for restricted object and file types	Must Have
3.71	The proposed Solution should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic	Must Have

	information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.	
3.72	The proposed Solution should conceal any HTTP error messages from users	Must Have
3.73	The proposed Solution should remove application error messages from pages sent to users	Must Have
3.74	The proposed Solution should prevent leakage of server code	Must Have
3.75	The proposed Solution should support XPATH injection	Must Have
3.76	The proposed Solution should support RSS/Atom feed injection	Must Have
3.77	The proposed Solution must support a flexible set of follow-up actions to be taken in the event of an alert generation. For example, if an alert is generated based on a Policy, send an email to Administrator X and Manager Y followed by sending a syslog to Destination 1 and a CEF-formatted log to Destination 2.	Good to have
3.78	Should support manual/offline as well as automatic online updates of the Signatures & updation should be not cause any downtime	Must Have
3.79	Signature updation should be independent of the underlying firmware OS	Must Have
3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	Good to have
4	**Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation**	
4.1	Proposed Solution should protect against OWASP Top-20 Automated threats for Applications. (The bidder should describe how each of the OWASP Top 10 Automated threats protection is addressed by the solution).	Must Have
4.2	The proposed solution should have the capability to proactively identify bots.	Must Have
4.3	The solution should be 100% automated and should not require bot-specific resource (from the organization) to manage the solution.	Must Have
4.4	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot h. Custom business logic	Must Have
4.5	The Solution must be able to Detect below types of Bad Bots: a. Misbehaving Legitimate Bots b. Bot Attacking from Public Cloud c. Known bad Bots d. Scripted Bots e. Programmatic session behavior. f. Advance Java Script validation Failure g. Malicious Browser Behavior h. Emulator tools i. Low and Slow Attacks j. Malicious intent detections~~:~~	Must Have
4.6	The Solution must be based on Intent oriented and User behavior Oriented	Must Have
4.7	The Solution must able to detect below type of attacks created by Bad Bots. a. Account take over b. Web Scrapping c. Application DDoS	Must Have

	e. Form Spam f. API Abuse	
4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	Must Have
4.9	The system must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such that: a. Slowloris b. Slow Post d. HTTP GET/POST Flood	Must Have
4.10	The proposed solution should protect against Ability to allow only specific HTTP Methods.	Must Have
4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Must Have
4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Must Have
4.13	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	Must Have
4.14	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.	Must Have
4.15	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup	Must Have
4.16	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.	Must Have
4.17	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.	Must Have
4.18	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention.	Must Have
4.19	Proposed WAF Solution should be able to provide a threat intelligence feed and service for bots protection & should be able to carry out Bot Classification of traffic into humans, Trusted Bot, Bad Bot, General Bot and Unknown new bot - Bot Type: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS Tool	Must Have
5	**API Security**	
5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Must Have
5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	Must Have
5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	Good to have

6	**High Availability**	
6.1	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR Environments.	Must Have
6.2	Should support seamless failover between devices in active-active/ active-standby, the failover should be transparent to other networking devices with SSL session mirroring capabilities	Must Have
6.3	Should support network based failover for session mirroring, connection mirroring and heartbeat check	Must Have
6.4	Device level HA should support automatic and manual synchronization of configuration from primary device to secondary device & vice-versa.	Must Have
6.5	Proposed solution should provide SSL offloading with the TCP connection and persistence session mirroring during the HA failover for all connections so that TCP connections are not lost during a failover event.	Must Have
7	**Server & Application health check features**	
7.1	Should provide individual health check for each Link and In case of link failure device should detect it in not more than 30 seconds	Must Have
7.2	Should be able to do health check on protocols like HTTP, HTTPS, SMTP, POP, TCP Ports etc.	Must Have
7.3	Should provide AND , OR mechanisms between multiple health checks	Must Have
8	**Monitoring, Logging & Reporting**	
8.1	Solution must support SNMPv2c, SNMPv3 & The system shall be capable of logging security events with Syslog.	Must Have
8.2	Proposed solution should have the detailed Access logs, Change logs for audit trail purpose	Must Have
8.3	The system must provide built in logging to 3rd party security event tracking systems such as SIEM like Arcsight, Splunk, Remote Syslog, IPFIX etc.	Must Have
8.4	The system must equip with a high-speed logging mechanism which can send log message in near real-time without significantly impacting system performance. (Logging around 15000 EPS, full logging)	Must Have
8.5	The solution should also support sending of logs in CEF (Common Event Format) standard	Must Have
8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Must Have
8.7	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables specification of a response to be issued when a specific requests/responses occur.	Must Have
8.8	The system must provide response logging so that it helps in analyzing responses is especially useful when logging response-related security events, such as Data Guard or response signatures, it is also be useful in analyzing request violations, to determine whether they represent an actual attack or a false positive	Must Have
8.9	The system shall have ability to generate service and system statistics. Provides dashboard displays anomaly statistics about number attacks, dropped requests, a summary of system traffic.	Must Have
8.10	The system must provide high-level view of recent activity in a single screen, where you can view aggregated events (incidents) rather than individual transactions (that are displayed on the Requests screen). Incidents are suspected attacks on the application.	Good to have
8.11	The system shall have ability to identify and notify system faults and loss of performance (over SNMP, syslog, e-mail, etc)	Must Have
8.12	The system shall be capable of logging security events with SNMP as well as SNMP MIB is polled for information about any current active attacks	Must Have
8.13	The proposed solution should have the capability to capture tcpdump, packetcapture for forensic analysis.	Must Have
8.14	The proposed solution should have the capability to create a granular logging policy per application.	Must Have

8.15	The system shall have ability to customize logging. The proposed solution should have the capability to define a customized log format for each application.	Must Have
8.16	The proposed solution should have the capability to define multiple log destinations for each application	Must Have
8.17	The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration: a. Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types) b. Daily & weekly Top 10 WAF violations c. Daily Summary Blocked Connections d. Data Leakage Report e. Directory Browsing Detection Report f. List of Alerts g. PCI - WAF violations h. Sensitive Error Messages Leakage Report i. Slow HTTP/S Alerts	Good to have
8.18	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create custom report templates based on the existing out-of-the-box reports.	Must Have
8.19	The solution must support automatic generation of reports based on a defined schedule.	Good to have
8.20	The solution must support scheduling of report generation to start only at a future date.	Good to have
9	**Administration**	
9.1	Proposed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts for accessing both CLI & GUI.	Must Have
9.2	Proposed Solution should have Role-based management & Access Control with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest	Must Have
9.3	Proposed solution should have Web GUI (HTTPS) for management. The solution must allow the user to use a standard browser to access the management UI	Must Have
9.4	Proposed solution should have CLI (SSH) for management	Must Have
9.5	Proposed solution should have the capability to restrict Web GUI/SSH from specific IP address	Must Have
9.6	Proposed solution should have the capability to restrict Shell access to specific users	Must Have
9.7	Proposed solution should have the capability to define separate ACL's for Web/SSH access	Must Have
9.8	The system must support Network Time Protocol (NTP) to synchronize its clock with an NTP server	Must Have
9.9	The entire solution must be centrally managed for day to day operations. The management server must centrally manage all the appliances. Reporting, policy creation, alerts management, web	Must Have

	application protection configuration, etc must be managed from the management server.	
9.10	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)	Must Have
9.11	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a. Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b. Number of failed login attempts which result an account to be locked c. Lock duration in minutes	Must Have
9.12	The solution must support the capability of trust-based communication between the different components in the solution. i.e. Communication between solution components needs to be done using certificates. Communication between Management server & WAF should be over a secure channel (Encrypted)	Must Have
9.13	The solution must allow administrators to add custom signatures and modify signatures	Must Have
10	**Licensing & support**	
10.1	Licensing structure proposed considering WAF Throughput, scalability & centralized architecture. The bidder has to provide the Enterprise (Premium) level licenses to cover all the features desired in the SOW including functional & technical requirements mentioned in this RFP	Must Have
10.2	Product manuals, trainings and user guides should also be provided along with the software as mentioned in this RFP.	Must Have

In case any of the above requirements are not generic in nature, it may be brought to the notice of NPCI through pre-bid mechanism.

Dated this…………………… Day of………………………..2021

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Section 10 - Documents forms to be put in Folder A

Annexure A1 - Bidder's Letter for EMD

To

The Chief Executive Officer
National Payments Corporation of India,
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Subject: RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021 for "Request for Proposal for Web Application Firewall Solution".

We have enclosed an EMD in the form of a RTGS - UTR No/BG No. ____ issued by the branch of the ____________Bank, for the sum of Rs. _____ (Rupees _____). This EMD is as required by clause 5.6 of the Instructions to Bidders of the above referred RFP.

Thanking you,

Yours faithfully,

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

Annexure A2 - Bid Security (Bank Guarantee)

____
[Bank's Name, and Address of Issuing Branch or Office]

National Payments Corporation of India: __________________

Date: _______________

BID GUARANTEE No.: ________________

We have been informed that________________ (hereinafter called "the Bidder") has submitted to you its bid dated (hereinafter called "the Bid") for the execution of __________________under RFP No.

Furthermore, we understand that, according to your conditions, bids must be supported by a bank guarantee.

At the request of the Bidder, we _____________ hereby irrevocably undertake to pay you without any demur or protest, any sum or sums not exceeding in total an amount of Rs.______/-(Rupees ______ only) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) Has withdrawn its Bid during the period of bid validity specified by the Bidder in the Form of Bid; or

(b) having been notified of the acceptance of its Bid by NPCI during the period of bid validity, (i) fails or refuses to execute the Contract document; or (ii) fails or refuses to furnish the performance security, if required, in accordance with the Instructions to Bidders.

This guarantee will expire:

(a) If the Bidder is the successful bidder, upon our receipt of copies of the contract signed by the Bidder and the performance security issued to you upon the instruction of the Bidder; or

(b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder of the name of the successful bidder; or (ii) twelve months after the expiration of the Bidder's Bid.

Consequently, any demand for payment under this guarantee must be received by us at the Office on or before that date.

____
[Signature]

Annexure A3 - Bid Security

(PERFORMANCE BANK GUARANTEE FORMAT)

Date:

Beneficiary: NATIONAL PAYMENTS CORPORATION OF INDIA
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Performance Bank Guarantee No:
We have been informed that------------------- (hereinafter called "the Supplier") has received the purchase order no. "------------------" dated -------------- issued by National Payments Corporation of India (NPCI), for -- (hereinafter called "the Purchase Order").

Furthermore, we understand that, according to the conditions of the Purchase order, a Performance Bank Guarantee is required to be submitted by the Supplier to NPCI.
At the request of the Supplier, We ------------------(name of the Bank , the details of its incorporation) having its registered office at --- and, for the purposes of this Guarantee and place where claims are payable, acting through its ---- branch presently situated at --- (hereinafter referred to as "Bank" which term shall mean and include, unless repugnant to the context or meaning thereof, its successors and permitted assigns),hereby irrevocably undertake to pay you without any demur or objection any sum(s) not exceeding in total an amount of Rs.---------------- (in figures) (Rupees--------(in words)------- only) upon receipt by us of your first demand in writing declaring the Supplier to be in default under the purchase order, without caveat or argument, or your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Please note that you may, if you so require, independently seek confirmation with –(Bank Name & Issuing branch address)---, that this Bank Guarantee has been duly and validly issued.

Notwithstanding anything contained in the foregoing:
The liability of ------------- (Bank), under this Bank Guarantee is restricted to a maximum total amount of Rs. ---------- (Amount in figures and words).
This bank guarantee is valid upto ------------------.
The liability of --------- (Bank), under this Bank Guarantee is finally discharged if no claim is made on behalf of NPCI within twelve months from the date of the expiry of the validity period of this Bank Guarantee.
Our liability pursuant to this Bank Guarantee is conditional upon the receipt of a valid and duly executed written claim or demand, by ---------- (Bank)--- (Address), delivered by hand, courier or registered post, or by fax prior to close of banking business hours on ------------- (date should be one year from the date of expiry of guarantee) failing which all rights under this Bank Guarantee shall be forfeited and -------------- (Bank), shall stand absolutely and unequivocally discharged of all of its obligations hereunder.

This Bank Guarantee shall be governed by and construed in accordance with the laws of India and competent courts in the city of Mumbai shall have exclusive jurisdiction.

Kindly return the original of this Bank Guarantee to -- (Bank & Its Address), upon (a) its discharge by payment of claims aggregating to Rs. -------- (Amount in figures & words); (b) Fulfillment of the purpose for which this Bank Guarantee was issued; or (c) Claim Expiry Date (date should be one year from the date of expiry of this Bank Guarantee).
All claims under this Bank Guarantee will be payable at --- (Bank & Its Address).

{Signature of the Authorized representatives of the Bank}

Annexure B - Bid Offer Form (without Price)

(Bidder's Letter Head)

OFFER LETTER

Date:

To
The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

Subject: RFP No. RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021 for "Request for Proposal for procurement of Web Application Firewall Solution".

We have examined the above referred RFP document. As per the terms and conditions specified in the RFP document, and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
We acknowledge having received the following addenda / corrigenda to the RFP document.

Addendum No. / Corrigendum No.	Dated

While submitting this bid, we certify that:

1. Prices have been quoted in INR.

2. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP.

3. We have not induced nor attempted to induce any other bidder to submit or not submit a bid for restricting competition.

4. We agree that the rates / quotes, terms and conditions furnished in this RFP are for NPCI and its Associates.

If our offer is accepted, we undertake, to start the assignment under the scope immediately after receipt of your order. We have taken note of Penalty clauses in the RFP and agree to abide by the same. We also note that NPCI reserves the right to cancel the order and order cancellation clause as per terms and condition would be applicable. We understand that for delays not attributable to us or on account of uncontrollable circumstances, penalties will not be levied and that the decision of NPCI will be final and binding on us.

We agree to abide by this offer till 180 days from the last date stipulated by NPCI for submission of bid, and our offer shall remain binding upon us and may be accepted by NPCI any time before the expiry of that period.

Until a formal contract is prepared and executed with the selected bidder, this offer will be binding on us. We also certify that the information/data/particulars furnished in our bid are factually correct. We also accept that in the event of any information / data / particulars are found to be incorrect, NPCI will have the right to disqualify /blacklist us and forfeit bid security.

We undertake to comply with the terms and conditions of the bid document. We understand that NPCI may reject any or all of the offers without assigning any reason whatsoever.

As security (EMD) for the due performance and observance of the undertaking and obligation of the bid we submit herewith RTGS/BG bearing no. ________ dated _________ drawn in favor of “National Payments Corporation of India” or Bank Guarantee valid for ____ days for an amount of Rs._____ (Rs. _____ only) payable at Mumbai.

Yours sincerely,

Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Company/Firm:
Address

Annexure C - Bidder Information

(Bidder's Letter Head)

Details of the Bidder				
1	Name of the Bidder			
2	Address of the Bidder			
3	Constitution of the Company (Public Ltd/ Pvt Ltd)			
4	Details of Incorporation of the Company.	Date:		
		Ref #		
5	Valid Sales tax registration no.			
6	Valid Service tax registration no.			
7	Permanent Account Number (PAN)			
8	Goods & Services Tax (GST) Registration Numbers			
9	City			
10	State			
11	Pin Code / State Code			
12	GSTIN Number			
13	HSN Number			
14	Name & Designation of the contact person to whom all references shall be made regarding this tender			
15	Telephone No. (Cell # and Landline # with STD Code)			
16	E-Mail of the contact person:			
17	Fax No. (with STD Code)			
18	Website			
Financial Details (as per audited Balance Sheets) (in Cr)				
19	Year	**2018-19**	**2019-20**	**2020-21**
20	Net worth			
21	Turn Over			
22	PAT			

Dated this…………………… Day of………………………..2021

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure D - Declaration for Clean Track Record

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the Terms & Conditions contained in the **RFP for procurement of Web Application Firewall Solution - RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021.** I hereby declare that my company has not currently been debarred/black listed by any Government / Semi Government / Private organizations in India / abroad. I further certify that I am competent officer and duly authorized by my company to make this declaration.

Yours faithfully,

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

Annexure E - Declaration for Acceptance of RFP Terms and Conditions

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP for procurement of Web Application Firewall Solution - RFP No. NPCI/RFP/2021-22/IT/12 dated 17.11.2021 I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

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

Annexure F - Declaration for Acceptance of Scope of Work

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the Scope of Work contained in the RFP for procurement of Web Application Firewall Solution - **RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021.** I declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

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

Annexure G - Format Power of Attorney

(On Stamp paper of relevant value)

Know all men by the present, we ________________________________ (name of the company and address of the registered office) do hereby appoint and authorize _________________ (full name and residential address) who is presently employed with us holding the position of ______________________ as our attorney, to do in our name and on our behalf, deed and things necessary in connection with or incidental to our proposal for ________ in response to the RFP for **procurement of Web Application Firewall Solution - RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021** by NPCI, including signing and submission of all the documents and providing information/responses to NPCI in all the matter in connection with our bid. We hereby agree to ratify all deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all deeds and things done by our aforesaid attorney shall always be deemed to have been done by us.

Dated this ______ day of ______ 2021.
For ________________________________.

(Signature)

(Name Designation and Address)

Accepted

(Signature)
(Name Designation)
Date:
Business Address:

Annexure H - Eligibility Criteria Compliance

(Bidder's Letter Head)

A] Start-ups:

Sr. No	Eligibility Criteria	Compliance (Yes/No)	Documentary proof to be attached
1	The bidder should be incorporated or registered in India under Companies Act/Partnership Act / Indian Trust Act (Annual filling with ROC) and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with NPCI.		1.Certificate of incorporation 2.MSME registration certificate (if applicable) 3. DPIIT Certificate
2	The bidder's annual turnover should be less than Rs. 100 crores as per audited financial statements in each of the financial years from the date of registration/ incorporation subject to compliance to Sr. No. 3		1. Standalone **audited** financial statements for last 3 years a. Balance sheets b. Profit /loss statement c. Signed Statutory Auditor's Report d. Notes to Accounts and Schedules forming part of accounts to be submitted. •*Complete financial statements duly signed/ approved by Auditor*. 2. CA certificate in case more than 3 years for previous years
3	The date of incorporation of the bidder should be anywhere between 1 to 10 financial years.		Certificate of incorporation/ registration
4	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self- declaration along with extract of auditors' report.		Self-declaration to be provided by the Bidder
5	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad.		Declaration letter from the **Bidder** and **OEM** as per **Annexure D**
6	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Authorization from OEM as per **Annexure I** Self-declaration of not being part of distribution channel

7	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission in case the bid document is downloaded from the NPCI website.		Remittance proof of RTGS in favor of NPCI
8	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of RTGS/ BG in favor of NPCI
9	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.		OEM Authorization letter to be provided

B] Other than Start-ups:

Sr. No.	MSME	Other than MSME	Compliance Yes/No	Documentary proof to be attached
1.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last three (3) years. a) In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least two (2) years as on date of submission of the bid. b) In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least two (2) years as on the date of submission of bid.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last five (5) years. a) In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least five (5) years as on date of submission of the bid. b) In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least five (5) years as on the date of submission of bid.		1. Certificate of incorporation 2. MSME registration certificate (if applicable)

2.	The bidder should have reported minimum annual turnover of **Rs. 6 crores** and should have **reported profits (profit after tax**) as per audited financial statements in at least **2 out of last 3 financial years** In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	The bidder should have reported minimum annual turnover of **Rs. 15 crores** in each of the last **3** financial years and should have reported profits (profit after tax) as per audited financial statements **in last 3 financial years.** In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.		Standalone financial **audited** financial statements 1. Balance sheets 2. Profit/ loss statement 3. Signed Statutory Auditor's Report 4. Notes to Accounts and Schedules forming part of accounts to be submitted.

3	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.		Self-declaration to be provided by Bidder
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad		Declaration from OEM as per Annexure D on company letter head Declaration from Bidder as per Annexure D on company letter head
5.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Declaration from OEM (as per Annexure-I) Self-declaration by bidder of not being part of distribution channel
6.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission in case the bid document is downloaded from the NPCI website.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission in case the bid document is downloaded from the NPCI website.		Remittance proof of Electronic Transfer in favor of NPCI
7.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of Electronic Transfer/ BG in favor of NPCI
8.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.		Self-declaration to be provided along with customer references

Dated this…………………… Day of………………………..2021

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure I - OEM / Manufacturer's Authorization Letter

[The Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. The Bidder shall include it in its bid]

Date:

To:

WHEREAS

We__________________________, are official manufacturers/OEM vendors of__________________. We________________ do hereby authorize M/S________________ to submit a bid the purpose of which is to provide the following Goods, manufactured by us ______________, and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty, with respect to the Goods offered by the above firm.

Signed by the Manufacturer/OEM Vendor:

Name:

Title:

Seal:

Dated on ____________ day of ___________________, _______

Section 11 - Documents to be put in Envelope/Folder 'B'

(Bidder's Letter Head)

Annexure J - Technical Compliance

Sr. No.	Specifications for Web Application Firewall	Requirement	Compliance (Yes/No)
1	**General Features & Requirements**		
1.1	The WAF Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for "Web Application Firewall" solution, or Forrester wave report for "Web Application Firewall" in leaders or strong performers category consecutively for last Two years (Two of last 3 years).	Must Have	
1.2	The vendor/bidder must be Gold/Tier-1 or Silver/Tier-2 or Authorized partner of the OEM for the proposed product.	Must Have	
1.3	The bidder should have back to back arrangement with the OEM so that NPCI will be able to log a call with the OEM directly.	Must Have	
1.4	The bidder should have support offices in Mumbai, Hyderabad and Chennai.	Must Have	
1.5	The bidder should have minimum 2 skilled OEM certified staff (Web Application Firewall - Subject Matter Experts) for the product proposed.	Must Have	
1.6	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Full Proxy mode (Should support Inline, reverse proxy, one armed reverse proxy & transparent reverse proxy, OOP Out of path modes of deployment)	Must Have	
1.7	There must be minimal impact on the existing applications and the network architecture when deploying or removing the solution from the network.	Must Have	
1.8	The Proposed Solution should have capability to deploy/integrate in Virtualized Environment/Opensource environments - Openstack, LinuxKVM etc.	Must Have	
1.9	The proposed solution should provide integrated functionalities of server load balancer, SSL Offloading, SSL Bridging.	Must Have	
1.10	The proposed solution must support TCP multiplexing, TCP optimization and dynamic Service chaining for SSL Offload with TCP session mirroring and persistence mirroring, compression, caching etc. in active-passive mode.	Must Have	
1.11	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed WAF should be capable to trigger a script based on an event	Good to have	
1.12	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration	Must Have	
1.13	The Proposed Solution should have option be manageable from a single management platform, Single management platform to manage policies across DC & DR.	Good to have	
1.14	The proposed solution should have a feature to generate device snapshot reports which then should be uploaded to an OEM provided online tool and get feedback on the health of the unit & missing Hotfixes and best practices	Must Have	
1.15	The proposed solution should provide minimum of 3 Gbps WAF Throughput per instance from day one (With all WAF functions enabled per instance in blocking mode) with sub millisecond latency.	Must Have	
1.16	The Proposed Solution should have support for multiple VLANs with tagging capability	Must Have	

1.17	The Proposed Solution should have capability to support minimum 50000 https Concurrent Connections scalable to 100000 https Concurrent Connections.	Must Have	
1.18	The proposed virtual solution Licenses should be independent of the hardware/platform/OS on which it is deployed & can be re-deployed at any other hardware/platform/OS if required.	Must Have	
1.19	Should support IPv4 & IPv6 addressing, IPv6 client and IPv4 servers with NAT44/NAT66/NAT64/NAT46 with full support for IPv6	Must Have	
1.20	Should support routing protocols RIP, OSPF and BGP to participate in Dynamic routing	Good to have	
1.21	Should have ability to upgrade/downgrade device software Images.	Must Have	
1.22	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.	Must Have	
2	**SSL/TLS Handling**		
2.1	The proposed solution should facilitate SSL handling.	Must Have	
2.2	The system must be able to establish SSL session before sending any packet to backend servers	Must Have	
2.3	The system must support elliptic curve cryptography (ECC)	Must Have	
2.4	The system must support SSL/TLS client certificate authentication	Must Have	
2.5	The system should support TLS v1.1, v1.2, TLS v1.3, SSL v2 & SSL v3 (Highest version available)	Must Have	
2.6	Proposed solution should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for each application service	Must Have	
2.7	The system must store the certificate private key using a secure mechanism (With & without passphrase)	Must Have	
2.8	The system must capable of communication with the original backend application server / Application service over SSL or TLS. should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL/TLS connection to the backend server	Must Have	
2.9	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.	Must Have	
2.10	Proposed solution should be able to integrate with external SSL visibility solution i.e. F5, radware etc.	Must Have	
3	**Web Application Firewall**		
3.1	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.	Must Have	
3.2	Proposed solution should be ICSA Lab Certified WAF	Good to have	
3.3	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution).	Must Have	
3.4	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions to address the compliances and configure policies for it.	Must Have	
3.5	When deployed as a full proxy mode, the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.	Must Have	

3.6	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	Must Have	
3.7	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over.	Must Have	
3.8	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat Sentinel, IBM Appscan, Rapid7-Nexpose, tenable-Nessus and QualysGuard, for rapid virtual patching.	Must Have	
3.9	The solution must be able to validate encoded data in the HTTP traffic	Must Have	
3.10	The solution must be able to identify Web Socket connections and provide security for WebSocket including security for exploit against Server abuse, login enforcement, XSS and SQL injection. The Solution must be able to parse and monitor JSON data over web socket protocol	Must Have	
3.11	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	Must Have	
3.12	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.	Must Have	
3.13	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	Must Have	
3.14	The Proposed Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions	Must Have	
3.15	The Proposed Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.	Must Have	
3.16	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.	Must Have	
3.17	The Proposed WAF Solution Should support ICAP, API or other supporting integration with different security devices for file scanning, sandboxing requests etc (industry leading security solutions i.e Symantec, McAfee, Trend Micro etc)	Must Have	
3.18	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Must Have	
3.19	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Must Have	
3.20	Proposed Solution should have ability to automatically detect application platform and its technology used on backend side to define signature sets required for defined Proposed Solution policy.	Must Have	

3.21	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy	Must Have	
3.22	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.	Must Have	
3.23	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.	Must Have	
3.24	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	Must Have	
3.25	Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc.	Must Have	
3.26	Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application	Must Have	
3.27	Proposed WAF Solution should have capability to learn changes in the already integrated Web Application & protect it at the same time i.e. solution should be able to learn changes in the application in the Protection Mode. Proposed Solution should have option to learn policy and configure the application in block mode simultaneously	Must Have	
3.28	The WAF Solution should have ability to configure application in block mode partially and learn the traffic for filters whose fine tuning is yet to be configured	Must Have	
3.29	Should be able to uniquely detect and block if required the end user on the basis of internal IP address, Plugins Installed in the browser, OS, Screen Resolution, Fonts etc. instead of going with traditional IP based blocking only	Must Have	
3.30	Solution should dynamically understand the Changes on the Web/Application Server	Must Have	
3.31	Should provide Policy creation per URL and not generic policy for URL’s	Must Have	
3.32	System should protects against the following threats/attacks: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Stealth commanding • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping • Directory/Path traversal • Remote File Inclusion	Must Have	

3.33	System supports enforcing policies regardless of character encoding in order to combat evasion techniques, WAF should support Policy Evasion Detection Engine to combat evasion techniques such as: • URL-decoding (for example, %XX) • Self-referencing paths (that is,. use of /./ and encoded equivalents) • Path back-references (that is, use of /../ and encoded equivalents) • Mixed case • Excessive use of whitespace • Comment removal (for example, convert DELETE/**/FROM to DELETE FROM) • Conversion of (Windows-supported) backslash characters into forward slash characters. • Conversion of IIS-specific Unicode encoding (%uXXYY) • IIS extended Unicode • Virtual directory route—positive folder enforcement • Base64 Encoded parameters & headers	Must Have	
3.34	The solution must provide the following features and protection: a. HTTP protocol validation b. Correlated based attack protection c. HTTP protocol attack signatures d. Cookie signing validation e. Anti-website scraping f. Whitelisting based protection g. Web worm protection h. Web application attack signatures i. Web application layer customized protection	Must Have	
3.35	The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP attacks g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. Parser protection (XML Bombs, Recursion Attacks)	Must Have	
3.36	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.	Must Have	
3.37	Should support XML Applications - solution must be able to protect web applications that include Web services (XML) content.	Must Have	
3.38	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.	Must Have	
3.39	The proposed WAF should support XML islands	Must Have	
3.40	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.	Must Have	

3.41	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)	Good to have	
3.42	The system must capable of blocking specific list of HTTP methods	Must Have	
3.43	The system must be able to allow or disallow specific file type	Must Have	
3.44	The system must be able to enforce specific HTTP headers and values to be present in client requests	Must Have	
3.45	The system must be able to perform information display masking/scrubbing on requests and responses	Must Have	
3.46	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user d. Block the IP address	Must Have	
3.47	The solution must be able to block the user or the IP address for a configurable period of time	Must Have	
3.48	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode	Good to have	
3.49	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2.	Must Have	
3.50	The solution must be able to decrypt SSL web traffic between clients and web servers	Must Have	
3.51	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	Must Have	
3.52	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	Must Have	
3.53	The solution must include a pre-configured list of comprehensive and accurate web attack signatures	Must Have	
3.54	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	Must Have	
3.55	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must have an option to be continuously and automatically updated	Must Have	
3.56	The solution must support regular expressions for the following purposes: a. Signatures definition b. Sensitive data definition c. Parameter type definition d. Host names and URL prefixes definition e. Fine tuning of parameters that are dynamically learnt from the web application profiles	Must Have	
3.57	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic	Must Have	
3.58	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP requests and responses, HTTP(S) headers, form fields, and the HTTP(S) body	Must Have	

3.59	The solution must be able to inject HTML snippet/text in the HTTP response	Must Have	
3.60	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header	Must Have	
3.61	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header	Must Have	
3.62	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	Must Have	
3.63	The solution must be capable to automatically create whitelisting/profiling of web applications.	Must Have	
3.64	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria.	Must Have	
3.65	The solution must be able to perform virtual patching for its protected web applications.	Must Have	
3.66	The solution must support the capability to define security policies based on the threat intelligence feeds listed previously to perform the following functions: a. Alert b. Block IP c. Block Session d. Block User	Must Have	
3.67	The proposed Solution should be session aware and should be able to enforce and report session	Must Have	
3.68	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.	Good to have	
3.69	The proposed Solution should be able to protect against Manipulation of invalidated input	Must Have	
3.70	The proposed Solution should protect against requests for restricted object and file types	Must Have	
3.71	The proposed Solution should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.	Must Have	
3.72	The proposed Solution should conceal any HTTP error messages from users	Must Have	
3.73	The proposed Solution should remove application error messages from pages sent to users	Must Have	
3.74	The proposed Solution should prevent leakage of server code	Must Have	
3.75	The proposed Solution should support XPATH injection	Must Have	
3.76	The proposed Solution should support RSS/Atom feed injection	Must Have	
3.77	The proposed Solution must support a flexible set of follow-up actions to be taken in the event of an alert generation. For example, if an alert is generated based on a Policy, send an email to Administrator X and Manager Y followed by sending a syslog to Destination 1 and a CEF-formatted log to Destination 2.	Good to have	
3.78	Should support manual/offline as well as automatic online updates of the Signatures & updation should be not cause any downtime	Must Have	
3.79	Signature updation should be independent of the underlying firmware OS	Must Have	

3.80	WAF should have capability to integrate with Database activity monitoring (DAM) tools for end-to-end security so as to protect/alert of any data breach/leakage by an attack or escalated privilege/admin rights, etc	Good to have	
4	**Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation**		
4.1	Proposed Solution should protect against OWASP Top-20 Automated threats for Applications. (The bidder should describe how each of the OWASP Top 10 Automated threats protection is addressed by the solution).	Must Have	
4.2	The proposed solution should have the capability to proactively identify bots.	Must Have	
4.3	The solution should be 100% automated and should not require bot-specific resource (from the organization) to manage the solution.	Must Have	
4.4	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot h. Custom business logic	Must Have	
4.5	The Solution must be able to Detect below types of Bad Bots: a. Misbehaving Legitimate Bots b. Bot Attacking from Public Cloud c. Known bad Bots d. Scripted Bots e. Programmatic session behavior. f. Advance Java Script validation Failure g. Malicious Browser Behavior h. Emulator tools i. Low and Slow Attacks j. Malicious intent detections:	Must Have	
4.6	The Solution must be based on Intent oriented and User behavior Oriented	Must Have	
4.7	The Solution must able to detect below type of attacks created by Bad Bots. a. Account take over b. Web Scrapping c. Application DDoS e. Form Spam f. API Abuse	Must Have	
4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network	Must Have	
4.9	The system must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such that: a. Slowloris b. Slow Post d. HTTP GET/POST Flood	Must Have	
4.10	The proposed solution should protect against Ability to allow only specific HTTP Methods.	Must Have	

4.11	system should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood	Must Have	
4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts	Must Have	
4.13	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	Must Have	
4.14	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify "good" and "bad" bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.	Must Have	
4.15	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup	Must Have	
4.16	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.	Must Have	
4.17	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.	Must Have	
4.18	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention.	Must Have	
4.19	Proposed WAF Solution should be able to provide a threat intelligence feed and service for bots protection & should be able to carry out Bot Classification of traffic into humans, Trusted Bot, Bad Bot, General Bot and Unknown new bot - Bot Type: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS Tool	Must Have	
5	**API Security**		
5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability for API is addressed by the solution).	Must Have	
5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration	Must Have	
5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	Good to have	
6	**High Availability**		
6.1	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR Environments.	Must Have	
6.2	Should support seamless failover between devices in active-active/ active-standby, the failover should be transparent to other networking devices with SSL session mirroring capabilities	Must Have	
6.3	Should support network based failover for session mirroring, connection mirroring and heartbeat check	Must Have	
6.4	Device level HA should support automatic and manual synchronization of configuration from primary device to secondary device & vice-versa.	Must Have	
6.5	Proposed solution should provide SSL offloading with the TCP connection and persistence session mirroring during the HA	Must Have	

	failover for all connections so that TCP connections are not lost during a failover event.		
7	**Server & Application health check features**		
7.1	Should provide individual health check for each Link and In case of link failure device should detect it in not more than 30 seconds	Must Have	
7.2	Should be able to do health check on protocols like HTTP, HTTPS, SMTP, POP, TCP Ports etc.	Must Have	
7.3	Should provide AND , OR mechanisms between multiple health checks	Must Have	
8	**Monitoring, Logging & Reporting**		
8.1	Solution must support SNMPv2c, SNMPv3 & The system shall be capable of logging security events with Syslog.	Must Have	
8.2	Proposed solution should have the detailed Access logs, Change logs for audit trail purpose	Must Have	
8.3	The system must provide built in logging to 3rd party security event tracking systems such as SIEM like Arcsight, Splunk, Remote Syslog, IPFIX etc.	Must Have	
8.4	The system must equip with a high-speed logging mechanism which can send log message in near real-time without significantly impacting system performance. (Logging around 15000 EPS, full logging)	Must Have	
8.5	The solution should also support sending of logs in CEF (Common Event Format) standard	Must Have	
8.6	There should be centralized Monitoring and Management station with capability for log collection as per Department log retention policy	Must Have	
8.7	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables specification of a response to be issued when a specific requests/responses occur.	Must Have	
8.8	The system must provide response logging so that it helps in analyzing responses is especially useful when logging response-related security events, such as Data Guard or response signatures, it is also be useful in analyzing request violations, to determine whether they represent an actual attack or a false positive	Must Have	
8.9	The system shall have ability to generate service and system statistics. Provides dashboard displays anomaly statistics about number attacks, dropped requests, a summary of system traffic.	Must Have	
8.10	The system must provide high-level view of recent activity in a single screen, where you can view aggregated events (incidents) rather than individual transactions (that are displayed on the Requests screen). Incidents are suspected attacks on the application.	Good to have	
8.11	The system shall have ability to identify and notify system faults and loss of performance (over SNMP, syslog, e-mail, etc)	Must Have	
8.12	The system shall be capable of logging security events with SNMP as well as SNMP MIB is polled for information about any current active attacks	Must Have	
8.13	The proposed solution should have the capability to capture tcpdump, packetcapture for forensic analysis.	Must Have	
8.14	The proposed solution should have the capability to create a granular logging policy per application.	Must Have	
8.15	The system shall have ability to customize logging. The proposed solution should have the capability to define a customized log format for each application.	Must Have	
8.16	The proposed solution should have the capability to define multiple log destinations for each application	Must Have	

8.17	The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration: a. Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types) b. Daily & weekly Top 10 WAF violations c. Daily Summary Blocked Connections d. Data Leakage Report e. Directory Browsing Detection Report f. List of Alerts g. PCI - WAF violations h. Sensitive Error Messages Leakage Report i. Slow HTTP/S Alerts	Good to have	
8.18	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create custom report templates based on the existing out-of-the-box reports.	Must Have	
8.19	The solution must support automatic generation of reports based on a defined schedule.	Good to have	
8.20	The solution must support scheduling of report generation to start only at a future date.	Good to have	
9	**Administration**		
9.1	Propsed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts for accessing both CLI & GUI.	Must Have	
9.2	Proposed Solution should have Role-based management & Access Control with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest	Must Have	
9.3	Proposed solution should have Web GUI (HTTPS) for management. The solution must allow the user to use a standard browser to access the management UI	Must Have	
9.4	Proposed solution should have CLI (SSH) for management	Must Have	
9.5	Proposed solution should have the capability to restrict Web GUI/SSH from specific IP address	Must Have	
9.6	Proposed solution should have the capability to restrict Shell access to specific users	Must Have	
9.7	Proposed solution should have the capability to define separate ACL's for Web/SSH access	Must Have	
9.8	The system must support Network Time Protocol (NTP) to synchronize its clock with an NTP server	Must Have	
9.9	The entire solution must be centrally managed for day to day operations. The management server must centrally manage all the appliances. Reporting, policy creation, alerts management, web application protection configuration, etc must be managed from the management server.	Must Have	

9.10	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)	Must Have	
9.11	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a. Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b. Number of failed login attempts which result an account to be locked c. Lock duration in minutes	Must Have	
9.12	The solution must support the capability of trust-based communication between the different components in the solution. i.e. Communication between solution components needs to be done using certificates. Communication between Management server & WAF should be over a secure channel (Encrypted)	Must Have	
9.13	The solution must allow administrators to add custom signatures and modify signatures	Must Have	
10	**Licensing & support**		
10.1	Licensing structure proposed considering WAF Throughput, scalability & centralized architecture. The bidder has to provide the Enterprise (Premium) level licenses to cover all the features desired in the SOW including functional & technical requirements mentioned in this RFP	Must Have	
10.2	Product manuals, trainings and user guides should also be provided along with the software as mentioned in this RFP.	Must Have	

The bidder is required to provide exhaustive list of the hardware, software, etc. to implement the project.
Dated this…………………… Day of………………………..2021

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure K - Client Reference

(Bidder's Letter Head)

NPCI/RFP/2021-22/IT/12 dated 17.11.2021

Sr.No	Particulars	Details
1	Name of the Organization	
2	Contact Person Name and Designation	
3	Phone Number of the Contact person	
4	Email Address of the Contact person	

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Section 12 - Documents to be put in Envelope/Folder 'C'

Annexure M - Commercial Bid Form

(Bidder's Letter Head)

(To be included in Commercial Bid Envelope/Folder)

To

NPCI

Dear Sirs,

Re: RFP # NPCI/RFP/2021-22/IT/12 dated 17.11.2021 for "Request for Proposal for procurement of Web Application Firewall Solution."

Having examined the Bidding Documents placed along with RFP, we, the undersigned, offer to provide the required infrastructure in conformity with the said Bidding documents for the sum of Rs.…………….(Rupees_____________) (exclusive of taxes) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to provide External Cyber Threat Intelligence Solutions within the stipulated time schedule. We agree to abide by the Bid and the rates quoted therein for the orders awarded by NPCI up to the period prescribed in the Bid which shall remain binding upon us. Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…………………… Day of……………………….2021

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

Annexure N - Commercial Bid

NPCI/RFP/2021-22/IT/12 dated 17.11.2021
RFP for procurement of Proxy Solution
(Bidder's Letter Head)

Table 1:

Sr. No.	Description	Qty	Equipment cost with 1 year onsite OEM warranty		AMC with support for 2nd Year		AMC with support for 3rd Year		Grand total (GT) (INR)
			Unit Price (INR)	Total Unit Price (INR)	Unit Price (INR)	Total Unit Price (INR)	Unit Price (INR)	Total Unit Price (INR)	
		A	B	C=A*B	D	E=A*D	F	G = A*F	T= (C+E+G)
1	Software/ Instance cost								
2	Implementation cost (if any)								
4	Others (if any, please specify)								
	Total (GT)								

- The bidder shall meet the requirements of Goods & Services Tax (GST)

(Amount in Rs)

All prices are exclusive of taxes.

Dated this…………………… Day of………………………..2021

(Signature)
(Name)
(In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure L - Bill of Material

NPCI/RFP/2021-22/IT/12 dated 17.11.2021
(Bidder's Letter head)

Line Item Wise Prices
(Details of all line items of the Commercial Bid)

Line Item	Item Name / Part No	Description	Unit Price including 1 year warranty and support	2nd Year-AMC with support	3rd Year-AMC with support	Sub Total	Quantity	Total Price
1								
2								
3								
4								
5								
5								
6								
Total (Exclusive of taxes)								

- Delivery locations would be as per clause 8.8 of the RFP

Annexure Z - Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT (NDA)

This Non-Disclosure Agreement ("**Agreement**") is made and entered on this ------- day of -------------, 2021 ("**Effective Date**") between

NATIONAL PAYMENTS CORPORATION OF INDIA, a company incorporated in India under Section 25 of the Companies Act, 1956 (corresponding to Section 8 of the Companies Act, 2013) and having its registered office at **1001A, B Wing, 10th Floor, The Capital, Plot 70, Block G, Bandra-Kurla Complex, Bandra (East), Mumbai - 400 051, Maharashtra**, CIN: U74990MH2008NPL189067 (Hereinafter referred to as "**Disclosing Party**", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

AND

______________________________________, a company/Partnership/Sole Proprietor/Association of People/ and having its registered office at ____ CIN;________________ (Hereinafter referred to as "**Receiving Party**", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

Disclosing Party and Receiving Party shall hereinafter be jointly referred to as the "Parties" and individually as a "Party".

NOW THEREFORE

In consideration of the mutual protection of information herein by the parties hereto and such additional promises and understandings as are hereinafter set forth, the parties agree as follows:

Article 1: PURPOSE

The purpose of this Agreement is to maintain in confidence the various Confidential Information, which is provided between Disclosing Party and Receiving Party to perform the considerations (hereinafter called "Purpose") set forth in below:

Purposes:

1.
2.
3.
4.
5.

Article 2: DEFINITION

For purposes of this Agreement, **"Confidential Information"** means the terms and conditions, and with respect to Disclosing Party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the Purpose (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the Receiving Party in violation of this Agreement); (ii) is lawfully acquired by the Receiving Party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the Receiving Party prior to its disclosure under this Agreement; (iv) was or is independently developed by the Receiving Party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case Receiving Party shall give the Disclosing Party prompt written notice, where possible, and use reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable the Disclosing Party to seek a protective order or other appropriate remedy at Disclosing Party's sole costs.

Article 3: NO LICENSES

This Agreement does not obligate the Disclosing Party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring to the Receiving Party any rights, license or authority in or to the Confidential Information disclosed to the Receiving Party under this Agreement or to any information, discovery or improvement made, conceived, or acquired before or after the date of this Agreement. No disclosure of any Confidential Information hereunder shall be construed to be a public disclosure of such Confidential Information by the Receiving Party for any purpose whatsoever. This Agreement does not create a joint venture or partnership between the parties.

Article 4: DISCLOSURE

1. Receiving Party agrees not to use the Disclosing Party's Confidential Information for any purpose other than for the specific purpose as mentioned in Article 1. Receiving Party agrees and undertakes that it shall not, without first obtaining the written consent of the Disclosing Party, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both parties may disclose any Confidential Information to their Affiliates, directors, officers, representatives, agents, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.
2. The Receiving Party shall use the same degree of care and protection to protect the Confidential Information received by it from the Disclosing Party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.
3. The Disclosing Party does not make any representation or warranty as to the accuracy or completeness of Confidential Information. The Disclosing Party shall not be in any way responsible for any decisions or commitments made by Receiving Party in relying on the Disclosing Party's Confidential Information.

Article 5: RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

The Receiving party agree that upon termination of this Agreement or at any time during its currency, at the request of the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Receiving Party or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

Article 6: INJUNCTIVE RELIEF

The Receiving Party hereto acknowledge and agree that it would be impossible or inadequate to measure and calculate the Disclosing Party's damages from any breach of the covenants set forth herein. Accordingly, the Receiving Party agrees that in the event of a breach or threatened breach by the Receiving Party of the provisions of this Agreement, the Disclosing Party will have no adequate remedy in money or damages and accordingly the Disclosing Party, in addition to any other right or remedy available, shall be entitled to injunctive relief against such breach or threatened breach by the Receiving Party and to specific performance of any such provisions of this Agreement. Disclosing Party shall be entitled to recover its costs and fees, including reasonable attorneys' fees, incurred in obtaining any such relief. If the Receiving Party is aware of a suspected or actual breach of this Agreement from Receiving Party's side, it shall (i) promptly notify the Disclosing Party in writing immediately; and (ii) take all reasonable and essential steps to prevent or stop any suspect or actual breach of this Agreement; (iii) Receiving Party shall cooperate with any and all efforts of the Disclosing Party to help the Disclosing Party regain possession of Confidential Information and prevent its further unauthorized use.

Article 7: NON-WAIVER

No failure or delay by either party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise of enforcement of any other right, remedy or power.

Article 8: DISPUTE RESOLUTION

Notwithstanding anything contained in Article 6 and the express rights of the Disclosing party contained and provided thereto, If any dispute arises between the parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 (or any statutory modification or re-enactment thereof and rules framed thereunder from time to time) by a sole arbitrator appointed by Disclosing Party Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the parties.

Article 9: GOVERNING LAW AND JURISDICTION

This Agreement shall be governed exclusively by the laws of India and jurisdiction shall be vested exclusively in the courts at Mumbai in India.

Article 10: NON-ASSIGNMENT

This Agreement shall not be amended, modified, assigned or transferred by Receiving Party without the prior written consent of Disclosing Party.

Article 11: TERM

This Agreement shall remain valid from the effective date till the time the Receiving Party is receiving Confidential Information or until the termination of this Agreement, whichever is later. This Agreement may be terminated by either Party by giving prior written notice of sixty (60) days to the other Party. However, the Receiving Party shall not be entitled to terminate this Agreement if there is subsisting business engagement between the Parties. Irrespective of the termination, the obligation of the Receiving Party to protect Confidential Information disclosed under this Agreement shall survive termination of this Agreement and shall remain in effect indefinitely.

Article 12: INTELLECTUAL PROPERTY RIGHTS, Media Disclosure, Publicity and Public Interaction

12.1 Receiving Party shall not use or permit the use of Disclosing Party's names, logos, trademarks or other identifying data, or infringe Patent, Copyrights or interact with media for any disclosure of findings or otherwise discuss or make reference to Disclosing Party in any notices to third Parties, any promotional or marketing material or in any press release or other public announcement or advertisement, however characterized, without Disclosing Party's prior written consent.

12.2 Any interaction by the Receiving Party with media for any disclosure of findings, publicity, public interactions for undue advantage and/or any association whatsoever of Disclosing Party, without express consent/approval from Disclosing Party, shall result in breach, and for every incident of breach the Receiving Party shall be liable to pay the Disclosing Party, an amount which Disclosing Party, in its sole and absolute discretion, deems fit. This shall be without prejudice to the right of Disclosing Party to peruse any other right or remedy available to it under law.

Article 13: INDEMNITY

In the event the Receiving Party discloses, disseminates or releases any Confidential Information received from the Disclosing Party, except as provided in this agreement, such disclosure, dissemination or release will be deemed a material breach of this Agreement and the Receiving Party shall stop its breach of this agreement immediately and indemnify Disclosing party against losses resulting from its default, including the reasonable legal costs, which have been incurred by Disclosing party to investigate the default.

Article 14: GENERAL

1. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third party.
2. Any notices or communications required or permitted to be given hereunder may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic-mail, or mailed by certified mail, return receipt requested, postage prepaid, in each case, to the address of the other party first indicated above (or such other addressee as may be furnished by a party in accordance with this paragraph). All such notices or communications shall be deemed to have been given and received (a) In the case of personal delivery or electronic-mail, on the date of such delivery, (b) In the case of delivery by a nationally recognized overnight carrier, on the third business day following dispatch and (c) In the case of mailing, on the seventh working business day following such mailing.
3. This Agreement and the confidentiality obligations of the Parties under this Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the parties with respect to the subject matter hereof and any additional agreement, if any, shall be binding along with that relevant Agreement in addition to this Non Disclosure Agreement without affecting the provisions of this agreement. In the event where only this agreement is existing than the provisions of this Agreement shall prevail. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement or modified, rewritten or interpreted to include as much of its nature and scope as will render it enforceable. The remaining provisions will continue in full force and effect.
4. Any breach of any provision of this Agreement by Receiving Party hereto shall not affect the Disclosing party's non-disclosure and non-use obligations under this Agreement.
5. The Parties agree that all Confidential Information shall remain the exclusive property of the Disclosing Party and its affiliates, successors and assigns.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement by their duly authorized representatives as of the Effective Date written above.

NATIONAL PAYMENTS CORPORATION OF INDIA	TYPE COMPANY NAME
By: Name:	By: Name:
Designation:	Designation: