Request for Proposal (RFP)

For

Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Bank's Data Centres

At

Reserve Bank of India

Tender ID:

RBI/DIT-CO Central Office Departments/Others/4/25-26/ET/178[IT Security Infra at Bank DCs]

Department of Information Technology

Reserve Bank of India

14th Floor, Central Office Building,

Shahid Bhagat Singh Road,

Mumbai-400 001

Disclaimer & Disclosures:

Reserve Bank of India, Department of Information Technology, Central Office, Mumbai, has prepared this document to give background information on the Project to the interested parties. While Reserve Bank of India has taken due care in the preparation of the information contained herein and believe it to be accurate, neither Reserve Bank of India nor any of its authorities or agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it.

The information is not intended to be exhaustive. Interested parties are required to make their own inquiries and respondents will be required to confirm in writing that they have done so and they do not rely only on the information provided by RBI in submitting RFP. The information is provided on the basis that it is non–binding on Reserve Bank of India or any of its authorities or agencies or any of their respective officers, employees, agents or advisors.

Reserve Bank of India reserves the right not to proceed with the Project or to change the configuration of the Project, to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the matter further with any party expressing interest. No reimbursement of cost of any type will be paid to persons or entities expressing interest.

The specification for components of the proposed solution is defined in generic terms on best effort basis. Reference of any term proprietary to an OEM in the RFP is incidental and has no other meaning other than specifying the nature and classification of the particular component of the proposed solution.

The proposal in response to the RFP should be signed and submitted by a person duly authorized to bind the bidding company to the details submitted in the proposal in response to the RFP. The signatory should give a declaration and through authenticated documentary evidence establish that he/she is empowered by the competent authority to sign the necessary documents and bind by the bidding. All pages of the RFP documents are to be signed by the authorized signatory. Any clarification sought can be mailed to below mentioned IDs. All clarifications sought shall be replied in pre-bid meeting or immediately thereafter through an addendum if necessary.

Contents

1. RFP Schedule and Important terms & conditions

The following table is an indicative time frame for the overall process. The Reserve Bank of India reserves the right to vary this time frame and/or venue at its absolute and sole discretion and without providing any notice/intimation or reasons thereof. Changes to the time frame and/or venue will be communicated to the Respondents concerned.

Indicative Time frame for the Overall Process is as shown below.

Sr. No.	Process	Date
1.	Issue of RFP Document	June 9, 2025
2.	Last date for receipt of queries over e-mail from bidders for Pre-Bid meeting	June 12, 2025, by 1500 hrs
3.	Date and Time of Pre-Bid Meeting	June 16, 2025, at 1130 hrs
4.	Date of publication of Addendum/ corrigendum to the RFP, if any	June 18, 2025
5.	Date & Time of Final Submission of Bids on the MSTC Portal	June 30, 2025, at 1100 hrs
6.	Date and Time of Technical Bid Opening	June 30 , 2025, at 1130 hrs
7.	Presentation to TAG	Will be communicated
8.	Date and Time of Commercial Bid Opening	Will be communicated
9.	Bid submitted by the Bidder will be valid for six months from the date of last date of submission of the Bid	180 days from the date of submission of bid

Contact details:

I.	Address for contact	Chief General Manager-in-Charge Department of Information Technology 14th Floor, Central Office Building, Reserve Bank of India, Shahid Bhagat Singh Road Mumbai - 400 001
II.	Contact Official and details	1. Shri Yogesh Dongre, Manager (Email: yogeshdongre@rbi.org.in, +91- 8830341331) 2. Shri Arun Sharma, Manager (Email: arunsharma1@rbi.org.in, +91 9717897923) 3. Smt Khushboo Panwar, Manager (Email: kpanwar@rbi.org.in) 022-22601000 Ext.- 2584
III.	Portal for registration of bidder on MSTC	https://www.mstcecommerce.com/eprocn/

Important Terms and Conditions

The Bid offers should be made strictly as per the formats specified in this RFP Document. The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Documents. Failure to furnish all information required by the Bidding Documents or submission of a bid not in conformity to the Bidding Documents in every respect will be at the Bidder's risk and may result in rejection of the bid.

The Bank at its discretion may reject the proposal of the Bidder without giving any reason whatsoever. All bidders are informed that the following **scenarios may lead to disqualification of bids.**

(i) The solution sizing is not made appropriately to meet the performance criteria as stipulated by the Bank and Bidder could not present or demonstrate the proposed solution as described in the proposal.

(ii) If the responses received from the reference sites are negative.

(iii) If the bidder/s is/are involved in any form of lobbying/ influencing/ canvassing etc., in the evaluation / selection process.

(iv) If the Technical Bid contain any pricing or commercial information.

(v) If commercial bid is not in line with the technical bill of material.

(vi) If Commercial Bid does not contain the prices/remarks for all the items indicated in the Technical BoM (without price) including any additional items proposed by the bidder.

(vii) If any rows or columns of the bid are left blank or zero price is quoted for any line item in the Bill of Material.

(viii) Bids with insufficient information which do not strictly comply with the stipulations given above.

The above list is only indicative in nature.

2. Introduction

2.1 Background

2.1.1 The Reserve Bank of India (RBI) (hereafter referred as RBI or "Bank") was established on April 1, 1935, in accordance with the provision of the Reserve Bank of India Act, 1934.

2.1.2 All the Data Centres of RBI located in the country will be covered under the scope of the proposed solution deployment. The indicative list is given in **Annex I.**

2.1.3 The Bank is building its own state-of-the-art, energy efficient, Greenfield Next Generation Data Centre (NGDC) which will be housed with latest technology. As part of our strategic initiative to establish a state-of-the-art data center in Bhubaneswar, we seek comprehensive proposals for designing and implementing advanced IT security infrastructure. Given the critical role of our data center in supporting our organizational operations and ensuring uninterrupted service delivery, it is imperative to build a robust, scalable, and secure network infrastructure. In this endeavour, Bank is seeking proposals for the procurement and implementation of advanced IT security infrastructure.

2.1.4 Reserve Bank of India invites proposals/bids in response to RFP for the following project:

"Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security infrastructure at Bank's Data Centres"

2.2 Purpose of Document

2.2.1 The Bank intends to sign a **five-year contract** with the selected Bidder/s of respective projects for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Bank's Data Centres"**.**

2.2.2 The Bank invites technically viable and commercially competitive proposals from the eligible bidders for the proposed solutions.

2.2.3 The Proposed Solution should also be integrated seamlessly with existing infrastructure at RBI.

2.2.4 A Bidder submitting the proposal in response to RFP for proposed solutions shall herein thereafter be referred to as "Bidder/Partner/Vendor/System Integrator" interchangeably.

2.2.5 This RFP is not an offer by the Bank, but an invitation to receive responses from the Bidders. No contractual obligation shall arise from the RFP process unless and until a Purchase Order is issued by Bank/formal contract is signed and executed by the duly authorized official(s) of the Bank with the selected Bidder.

2.2.6 RBI may modify any / all the terms of this RFP by giving due notification to all the bidders through RBI website and/or MSTC-Procurement Portal.

2.2.7 The Bank shall enter into a mutually agreeable contract with the Successful Bidder for the project. The RFP will be part of the contract as Annex.

2.2.8 The specification for components of the proposed solution is defined in generic terms on best effort basis. Reference of any term proprietary to an OEM in the RFP is incidental and has no other meaning other than specifying the nature and classification of the particular component of the proposed solution.

2.2.9 In case of a difference of opinion on the part of the Bidder in comprehending or interpreting any clause / provision of the Bid Document after submission of the Bid, the interpretation by the Reserve Bank and decision of the Reserve Bank in this behalf shall be final, conclusive, and binding on the Bidder.

3. Structure of RFP

This document consists of:

- An overview of services/requirements to be provided/fulfilled by the selected Bidder.
- Bidding process
- Evaluation methodology which shall be followed to select the successful Bidder for the projects.
- Terms and Conditions
- Annexes seeking response for evaluation.

4.Definition of Terms used in RFP

Definitions – Throughout this RFP/Bid Document/Contract, the following terms shall have the meanings as given below and shall be interpreted accordingly:

1. “RFP” means the request for proposal (this document) in its entirety, inclusive of any addenda/ corrigendum that may be issued by the Bank. RFP shall be part of the contract.
2. “Bank/Purchaser/Customer/RBI/Reserve Bank of India” means reference to “RBI”, “the Bank”, “Bank” and “Purchaser” shall be determined in context of this RFP.
3. “Proposal/ Bid” means the Bidder’s written reply or submission in response to this RFP.
4. “Services” means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and all ancillary services necessary for the supply, design, delivery at final destination, installation, implementation, integration, putting into satisfactory operation, support & comprehensive maintenance, project management and facilities management services (FMS).
5. “System” or “solution” means and includes hardware, software, etc., required for operationalising the proposed solution / Project and to provide the Services as mentioned in the RFP.
6. “Bidder/Service Provider/System Integrator/Vendor” means an eligible entity/firm submitting a Proposal/Bid in response to this RFP. The legal entity who signs and submit the bid.
7. “Successful Bidder” or “Vendor” means any firm / company, etc., to whom work has been awarded and whose Bid has been accepted by the Bank and shall include its authorized representatives, successors and permitted assignees.
8. “Acceptance of Bid” means the letter/email, or any memorandum communicating to the Bidder the acceptance of its Bid and includes an advance acceptance of his Bid.
9. “Agreement” means the contract signed between the Bank and the Selected Bidder(s) and all the attached documents. The “Agreement” includes the RFP, subsequent modifications to the RFP, response of the selected vendor to the RFP, clarifications requested from the bidder and the contract document itself.
10. “Audit, Validation & Certification by OEM”: The bidder is required to ensure that the competent team of OEM conducts an audit of implemented solution (production environment), in order to confirm that implementation and configuration has been done as per OEM best practices and the design is suitable to deliver 99.9 % uptime and required performance before Project-signoff.

11. “Contract Period” means the period of Supply, Design, Installation, Implementation, Integration and 5 years from the date of Project sign-off and onboarding and deployment of the requisite facility management resources.
12. 'Warranty’ means the period of 3 years from the date of Project sign-off and onboarding and deployment of the requisite facility management resources. During warranty period the bidder should maintain hardware and software components of the solutions and shall be responsible for all costs relating to its maintenance which includes all security upgrade for emerging threat and vulnerabilities.
13. Support & Comprehensive Annual Maintenance Contract (AMC) is a post warranty support of the project for Contract Period. Under AMC, the Bidder shall provide comprehensive support for hardware including maintenance, security upgrade for emerging threat and vulnerabilities of the proposed solution for 2 years after completion of 3-year warranty.
14. Annual Technical Support (ATS) is post general warranty support for comprehensive software maintenance. Under ATS, the Bidder shall provide comprehensive support including maintenance, security upgrade for emerging threat and vulnerabilities for software of the proposed solution for 2 years after completion of 3-year warranty.
15. “Authorised Signatory” means the person authorized by the Competent Authority of the respective company (say Board- in terms of applicable statutory provisions), for signing all the documents for purpose of this bid and to enter into contract thereafter, if successful in the bidding process. The documentary evidence to establish the identity and authority of authorized signatory must be submitted along with the bid document.
16. “Installation” or “Implementation” or “Commissioning” means the installation of equipment/software/appliance at the Banks’s premises or at such other location as may be specified by the Bank, implementation of which will be considered complete only after successful sanity testing and integration of all installed solutions with each other and other existing IT/Non-IT infrastructure including security layers/components.
17. “Operationalization” means when all the components of the proposed solution are successfully commissioned, implemented and tested. Thereafter, Certification by the respective OEMs that the components are in fully working condition to meet

day to day operational requirements and any demands placed upon those products.

18. “Site” means the place where the product / service / solution is to be delivered and commissioned or places approved by the Bank for the purposes of the Contract together with any other places designated in the Contract as forming part of the Site.
19. “One Time Cost” means cost which includes the cost of Supply (Hardware/Software), Design, Installation, Implementation and Integration of Hardware, software and any other required component for the proposed solution.
20. “Recurring Cost” means AMC/ATS for hardware, software, licenses, etc. plus, Resource/ FMS cost/ Services and any other recurring cost defined specifically.
21. “Uptime” of the project means the amount of time all the services are available and operational. Guaranteed required uptime as expressed in SLA is 99.9% level and calculated on quarterly basis.
22. “Incident” refers to any event / abnormalities in the functioning of any of the components of the “proposed solution” that may lead to disruption in normal operations.
23. “Availability” shall mean the time for which the services offered are available for conducting operations from the equipment / proposed solution hosted in RBI.
24. “Support" shall mean the 24x7 support which shall handle Change Management and resolution to Fault/incident Reporting, Trouble Ticketing, and related enquiries during this contract.
25. “Planned downtime / Scheduled downtime” shall mean any time when any of the subsystems/proposed solution are unavailable because of Urgent Maintenance activities and any other scheduled maintenance or upgrade activities that may or may not be periodic. The planned downtime must be notified to the Bank at least 48 hours in advance.
26. “Urgent Maintenance” activities are maintenance activities that cannot be postponed until the next available or convenient maintenance window, and may include but not limited to restarting applications, rebooting servers, applying patches or fixes, reconfiguring, reloading data etc.
27. “Response time” is defined as the time between receipt of the incident by support team and its logging / generation of ticket on the system.

28. “Restoration/Resolution Time” shall mean the time taken (after the incident has been reported to the support team) till resolution subject to the acceptance of the Bank.
29. “Delivery Completion” Delivery shall be considered completed on the Confirmation of delivery of all items as per Purchase Order and successful Power-On-Self-Test (POST) at respective sites.
30. Person day – 8 hours of work of a qualified person.
31. Person Month – 22 working days
32. Throughout Scope of Work (SOW), the following terms shall have the meanings as given below and shall be interpreted accordingly:
    a. “Design Workshop”: includes gathering Information from the bank about business, functional use cases, application flows, high availability, scalability and security policies.
    b. “Design Document” normally includes two documents:
        High Level Design (HLD): Blueprint to cover the banks requirements, End State Design, Traffic Flows and design recommendations.
        Low Level Design (LLD) that provides a physical layout, building blocks and policy templates in line with the High-Level Design.
    c. “Migration Strategy” Document – This document provides an agreed phase wise Go-Live Plan that is used by IT Operations, Project Management and Technical Team alike to plan the sequence of maintenance windows to migrate traffic and workloads from existing setup to the new setup.
    d. “Solution Readiness” Document – This document provides a list of test scenarios along with the procedure to replicate the scenarios and expected outcomes. The intent of the document is to validate and verify the deployed solution meets expected failover and functionality requirements.
    e. “Method of Procedure” (MOP) Document: This document lists down stakeholders’ activities during the migration window for both the Roll-Forward and the Roll Back Plans including estimated timelines for each of the tasks. It shall also list down configuration steps that engineer shall follow through the maintenance window.

5. Requirements and Scope of Work

5.1 Scope of Work

The Successful Bidder in Partnership with OEM shall Supply, Design, Install, Implement, Integrate, Support & Maintain, and provide comprehensive Facilities Management Services for IT Security Solutions as per the Project scope of the RFP during the entire contract period:

5.1.1 Bidder's Scope of Implementation (For all solutions)

S No	Responsibility
1	Bidder shall supply equipment procured through this RFP at Bank locations as per the delivery schedule.
2	Bidder shall verify equipment delivery as per bill of material approved by Bank.
3	Bidder shall carry out unpacking and physical verification of the supplied equipment and any physical movement of those equipment across Bank locations
4	Bidder shall supply and install racks as per respective RFP specifications. Also, bidder has to carry out physical installation (Racking and Stacking) of supplied equipment in allocated racks as per respective RFP specifications
5	All passive cabling for supplied component, including passive supply and installation, shall be included in bidder's scope.
6	Bidder shall supply Ethernet and Fibre cables for the supplied bill of material
7	Bidder shall carry out Structured Cabling for the supplied equipment, which includes supply of necessary cables, labelling, Dressing and tagging of Power Cables, Ethernet, Fibre Cables within the Rack & Inter-rack.
8	Bidder shall carry out documenting the planned and deployed equipment placement and cabling layouts
9	Bidder shall perform POST (Power ON Self-Test) for all supplied equipment's
10	Project management services - Bidder shall devise the implementation plan with clear and objective timeline. The implementation may be tracked using a standard IT Project Management Template like Gantt chart or timeline chart. Bidder shall be responsible to create, present and update a Unified Project Plan in consultation with Bank and OEM Project Manager to create a Unified Project Plan.
11	Bidder/OEM shall ensure implementation of all the bank's ordered hardware is completed as per timelines outlined in RFP.
12	The bidder shall supply, install, integrate, test and operationalize the solution as per the Indicative Bill of Material in **Annex IV** and as per the scope of implementation
13	Bidder shall ensure that OEM shall be responsible to Design, Configuration, Implementation, and Testing for supplied Equipment as part of this RFP
14	The bidder shall engage OEM services for plan, design and implementation of the solution. The bidder shall ensure that the OEM has end to end responsibility for plan, design, implementation, operationalization and sustenance of proposed solution under RFP

15	Bidder shall provide complete end to end solution including hardware, software, necessary accessories, active and passive components etc. for efficient functioning of the solution.
16	Bidder shall coordinate with the bank and the FMS team(s) managing the existing infrastructure, for any changes like re-configuration, implementation etc. if required on existing infrastructure and devices which are not supplied as a part of this RFP, if such activities are required for the execution of scope of work under this RFP.
17	Bidder shall be responsible for Unmounting / removing any equipment from the racks
15	Bidder shall be responsible for Packing of any existing equipment and any physical movement of those equipment across Bank locations if required for the execution of the scope of work.
16	Bidder shall provide Escalation Matrix for the overall project up to the level of CEO
17	Bidder's expert team shall be onsite till complete installation, implementation and project signoff.
18	Bidder shall ensure product support as per the scope of warranty/support
19	Additional hardware, software, accessories, active and passive components etc. if any required, for providing the 'Total solution' as envisaged in the RFP document shall be specified and quoted by the bidder. Required technical details/ brochure of all the products offered by the bidder duly supported by schematic diagrams and technical specifications of each component offered shall be furnished along with the reasons justifying the requirement/s for such additional components, accessories, active and passive components as part of the Technical Bid and the cost of each of such component/s shall be furnished in the Commercial Bid as per the format given in **Annex VI**
20	The successful bidder shall designate most experienced and qualified L3 as Project Manager for Supply, Installation, Testing and Commission (SITC) of complete solution. The Bank may get independent status report from the designated Project Manager. Successful Bidder needs to submit the progress report to bank in granular manner in a format agreed by the Bank
21	Selected Bidder has to do comprehensive site survey in coordination with Bank DCs and should analyse the actual requirement of all components and prepare the list for any additional bill of material required at all the locations and submit the report within 3 weeks of receiving purchase order. The report should also include requirements / suggestions for passive components, ports in switches, power supply etc. Based on the survey report addendum to Purchase / Work Order will be issued**.** The Bidder must deliver the equipment at the respective offices/ DCs. Also, dimensions, footprints, maintenance clearances, environmental conditions (temperature/RH) and weight of each piece of hardware equipment offered shall be specified with necessary power and wiring requirements in terms of the specified standards for these items in the country

22	Uninstallation of existing software, hardware and other equipment required to build the proposed IT security solution, installation and relocation of new/existing hardware, software and other infrastructure is under the scope of proposed solution.
23	**Project Implementation and Governance Teams** The shortlisted bidder shall formulate a Project Governance team and a dedicated Project Implementation team for this project, including appropriate representation from OEM and share details of the same with RBI. The details of these project teams shall be furnished along with technical bid. The shortlisted bidder shall formulate entirely separate governance and implementation team for existing Data centre implementation.
24	**Project Governance Team** – Governance Team shall comprise of the Project Manager, Project Director (should be from senior management from Bidder) and Service Delivery Head (preferably the national service delivery head); and will be responsible for reviewing and overseeing the project during implementation. Project governance meetings will be held at least once in a month during the implementation and on mutually decided interval post-implementation of the project on need basis.
25	**Project Implementation Team** – Implementation team shall comprise of Project Manager and SMEs from OEM(s). The team shall be responsible for implementation of the proposed solution as per the implementation schedule and scope

5.1.2 OEM's scope of implementation

S. No.	General Responsibilities
1	OEM shall be consulted for all the design and configuration related changes during the migration period for all OEM Devices (new as well as existing) across all Data Centres of Bank as required for migration.
2	OEM shall be responsible for the following Project Management Services for all OEM responsibilities, which include: a. Provide OEM project management services for all OEM responsibilities and work closely with bidder and Bank's project management team. b. Participate in scheduled project review Meetings and Conference calls c. Work with Bidder and Bank to identify and document dependencies, risks and issues associated with the project. d. Provide a project plan for implementation and migration and provide weekly updates on project progress jointly with the Bidder Project Management team.

3	The proposed OEM Data Centre Design, Implementation and Onboarding/Migration Services shall be applicable for all the supplied devices under this RFP
4	The OEM services team shall devise the implementation plan with clear and objective timeline. The implementation may be tracked using a standard IT Project Management Template like Gantt chart or timeline chart
5	The implementation team shall share the pre-requisites in terms of infrastructure readiness well in advance and co-ordinate with the Bank's IT Infrastructure Team to execute the necessary Change Request in order to optimise the project implementation schedule

5.1.2.1 OEM Data Centre Plan, Design and Implementation service

S. No.	Scope
1	Bidder and OEM services team shall conduct a workshop to gather the inputs of the Bank in relation to solution requirement with respect to the baselining and scoping of the components including but not limited to Solution architecture, sizing, policy configuration, High availability, DR scenarios etc. and provide the Solution Requirement Document.
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	Continuity of Banking operations are critical therefore OEM shall have to provide a mutually agreed Migration Strategy
4	Few design Scope as below: a) Includes all DC security devices proposed as part of this RFP b) Define DC Zoning and Traffic flows, such as Banking services, DMZ, External Business Partners (EBP), Secured and Non-Secured Branch Networks c) Plan the integration of supplied devices with existing Services such as Load Balancers, Firewalls, VPN Concentrators, IDS, IPS, WAF, DNS, NTP, TACACS, ITAM, etc
5	OEM shall draft an Acceptance Test Plan document including Readiness test cases and present for review to the bank
6	The OEM shall draft an Implementation Plan document based on the Solution Design Document (SDD) which captures the configuration necessary to prepare the devices for migration and operation.

7	Set up the logical configurations for all other products in accordance with the product specification
8	OEM shall implement and configure below solution components in Banks Data Centres (DCs): a) All products supplied under this RFP b) Verification of firmware, upgrade if needed c) DC Zoning and traffic flows such as Banking services, DMZ, MZ, External Business Partners (EBP), Secured and Non-Secured Branch Networks d) Integration with Services such as Load Balancers, Firewalls, VPN, IDS, IPS, WAF, DNS, NTP, TACACS, ITAM, etc. e) Integration with Bank's NOC tools such as AAA, RADIUS, Syslog and NMS tools. f) OEM and Bidder shall jointly execute the Readiness test cases along with the bank's team, as per approved Acceptance Test Plan Document. i) The Acceptance test Plan document, shall be mutually agreed upon and shall contain an objectively measurable criteria for final acceptance of the solution
9	OEM shall hand over the following documents to the Bank and FMS team: a) Solution Requirement Document b) High Level Design (HLD) c) Low Level Design (LLD) d) Acceptance Test Plan Document (ATP) e) Implementation Plan Document f) Onboarding/Migration Plan g) Standard Operating Procedure (SOP) wherever requested / needed
10	The Detailed Design Document shall include the following aspects: i. Technical objectives and requirement fulfilment. ii. High-level and low-level solution design requirements. iii. Design recommendations. iv. Proposed network, Security topology and Architecture. v. Network - Logical and Physical topology. vi. Security design. vii. Sample configuration templates for hardware devices and other devices for which configurations need to be made.

	viii. Hardware and Software release recommendations based on features and/or functionality. ix. The Design Document shall also document the management of DR scenarios and DR Drills of the solution. x. End-user manuals and SOPs, wherever applicable.
11	OEM(s) shall deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments
12	The implementation team shall provide the necessary templates for on-boarding of users/ log sources/ Active directory/ network & security devices/ other solutions etc. for various solutions for enabling overall integration. The configuration changes to implement these in production devices (device/ user on-boarding) shall be done by FMS teams maintaining these devices
	The Acceptance Test Plan shall also include: i. Testing of each hardware, software etc. listed in Bill of Material in Purchase Order for its working on expected lines. ii. Use cases need to be tested for working on expected lines subject to the feasibility of testing. iii. Testing results shall be documented with proper screenshots and necessary observations

5.1.2.2 Data Centre Onboarding/Migration Services, Testing, Validation and Certification of overall implementation

S. No	Scope
1	Continuity of Banking operations are critical therefore OEM shall provide a mutually agreed Method of Procedure (MOP) Document, including Roll-Forward and the Roll Back Plans.
2	OEM shall perform following services as part of onboarding/migration services: a) Jointly work with Bank's Application Owner's / Bank's Team to define Migration procedures. b) Build Method of Procedure (MOP) Document for the targeted application/s c) Carryout Onboarding/Migration activities as per MOP, Perform Configuration activities in Bank's Data Centre as per documented MOP and change management process d) Execution of Roll-back procedure in the event of Change failure e) Engage with OEM's Technical Assistance centre for any issues requiring Troubleshooting or Engineering Support observed before or during migration. f) Provide OEM incident management services to address any incidents/issues faced during the migration change windows.

	g) Post migration window the devices shall be handed over to the Bank's operations team.

5.1.3 Other requirements

i. With respect to devices proposed for current DCs (PDC, ODC, and DRDC), implementation of those devices shall be in accordance with existing security and network architecture, design, and policy in these DCs in coordination with FMS & OEM teams currently managing the network and security in these DCs.
ii. Implementation in Admin building in Bhubaneswar shall be in accordance with existing network and security architecture, design and policy in this building in coordination with FMS & OEM teams currently managing this building.
iii. Post completion of implementation of solutions/products procured under this RFP, the competent team of each OEM needs to conduct an individual audit of their respective implemented solution (production environment), to confirm that implementation, configuration, Onboarding/migration etc. has been done as per respective OEM's best practices and the design is suitable to deliver required uptime. Each OEM needs to submit a completion certificate to this effect for their respective solution implemented under this RFP.
iv. The solution shall be handed over to the FMS team after successful completion of acceptance testing as per the Acceptance Test Plan and the issuance of the 'Acceptance Certificate' by the RBI to the Bidder. The Acceptance Test plan post implementation shall incorporate the successful demonstration of proposed solution as per RFP.
v. OEM shall certify the bill of material for both, products and support, components on their letter head for all the equipment/ components including support components quoted by the bidders as per the requirement given in the RFP.
vi. The total solution shall undergo Bank's internal or third-party vulnerability assessment and other security and risk assessment before Go-Live. The successful bidder shall facilitate testing of the solution from security and process perspective and shall take complete responsibility to fix the gaps found in the security assessment before going live.
vii. The bidder and OEM services team shall handover the operations of the solution to the on-site FMS team with hands-on Knowledge Transfer Session and with very detailed Standard Operating Procedure (SOP) document
viii. The SOPs shall contain guidelines for FMS team to enable them to carry out the operations under the scope of FMS team including troubleshooting, security monitoring, incident management, change management and configuration management etc.
ix. The bidder and OEM services team shall provide a sample template to the FMS team with guidelines for on boarding of new users/ devices/ log sources/ tools

etc. The sample templates shall be prepared separately for all the applicable tools.

x. All the relevant documentation including SOPs, workflows, manuals etc. need to be submitted by the bidder for the total solution before handing over operations to the FMS team.

xi. An independent onsite comprehensive review by SMEs of each OEM (OEM experts/ Technical Architect from OEM for respective solution) for all the solutions shall be performed in coordination with bidder based on an objective Performance Metrics as decided by the Bank based on which the overall value addition, productivity and efficiency of each solution shall be finalised at the end of each year during the contract period (Ex: at least five times in the contract period of 5 years). This includes, but not limited to, review of hardware, software, solution architecture, integration, features, functionalities, patches, road map etc. **Any solution/ component resource not meeting the desired criteria shall be discontinued and replaced with the latest available solution/ component etc for remaining contract period**.

5.1.4 Solution-wise scope of implementation (For both OEM and bidder)

Next Generation Firewall & Sandboxing (Category A – Internal Firewall, Category B - External Firewall & Category C - Malware Sandboxing for External Firewall)

The Scope of work for firewall solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to proposed firewalls at respective locations. The Bank, now, proposes to purchase Next Generation Firewalls System for detecting and stopping malicious traffic as a preventive control solution.

The successful bidder will take total responsibility for providing and seamless commissioning the Firewalls into Banks network.

S. No.	Scope
1	Supply of appliance based Next Generation Firewalls with provision of version upgrades/patches.
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD).

3	Design, validate, installation, implementation as per Bank's IT security architecture design & pattern of traffic; this will include device rules / device policy definition and enforcement on the appliances proposed in this RFP.
4	Proposed firewall OEM/make shall be different for Category A - Internal Firewall and Category B - External Firewall. This RFP is to procure different make/OEM firewalls for Internal and External Firewall considering the best security practices of not using same make of firewall in adjacency in a row.
5	Performance tuning- Performance tuning so that the solution operates as proposed on the production network.
6	To provide licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
7	Return merchandise authorization (RMA) process for replacement of appliance to be completed within 24 hours from reporting time of issue.
8	Bidder shall provide the latest model in the class as per RFP requirement and the model shall not be declared end of sale within 24 months of delivery to the Bank. If the model gets declared end of sale within 24 months, then bidder shall provide latest firewall appliance with similar specification without any additional cost to Bank.
9	Bidder shall develop a Standard Operating Procedure (SOP) for alert management, incident management, forensics, report management, log storage and archiving, Business Continuity. SOP shall also cover log monitoring tool management including configuration, backup, and recovery.
10	Bidder shall provide knowledge transfer and training on the technology, functionality, and operations of the proposed firewall solution to current service integrator and Bank officials.
11	Any Team Lead change during implementation of the project shall be carried out only after mutual consent and shall comply with the RFP Eligibility criteria.
12	Bidder shall provide OEM trained resource with relevant certifications in the proposed solution for regular day to day operation and manage the same. In case of outage or critical activity i.e., periodic/ unplanned DR drill, resources shall be available 24/7 at Banks premise
13	The proposed sandbox solution for PDC, ODC & DRDC shall seamlessly integrate with existing production firewalls.
14	The proposed external firewall solution (Category B) for PDC, ODC & DRDC shall support comprehensive VPN functionalities and necessary licenses required if any shall be included by Bidder for the same.

Load Balancer

The Scope of work for Load Balancer solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to proposed Load Balancer (LB).

The successful bidder will be totally responsible for providing and seamless commissioning of the LB appliances into Banks network, as per the given configuration of existing devices.

S. No.	Scope
1	Supply of appliance-based Load Balancer with provision of version upgrades/patches.
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	Design, validate, installation, implementation as per Bank's IT security architecture design & pattern of traffic, this will include device rules / device policy definition and enforcement on the appliances proposed in this bid.
4	Installation of the proposed appliance will include migration of policies and configuration of the existing LB.
5	To provide licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
6	Bidder shall deliver, deploy, integrate & maintain LB appliances in Bank's premises for application availability and load distribution. Additionally, Bidder shall also provide OEM trained resource with relevant certifications in the proposed solution for regular day to day operation and manage the same. In case of outage or critical activity i.e., periodic/ unplanned DR drill, resources shall be available 24/7 at Banks premise.
7	Bidder shall provide the latest model in the class as per BID requirement and the model shall not be declared end of sale within 24 months of delivery to the Bank. If the model gets declared end of sale within 24 months, then the bidder shall provide latest LB appliance with similar specification without any additional cost to Bank.
8	There shall be minimal impact on the existing Web application and the network architecture when deploying or removing the solution from network.
9	The proposed solution for PDC, ODC & DRDC shall ensure uniformity in application architecture across PDC, ODC & DRDC.

Web Application Firewall (WAF)

The Scope of work for WAF solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to proposed WAF.

S. No	Scope
1	The Bidder shall supply, implement, and manage a WAF solution to identify and mitigate the OWASP Top10, API, CVE signatures TOP 25 and other qualified web applications, API based on vulnerabilities attacks and patterns and signatures, as per the guidelines issued by the Bank from time to time.
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	Bidder shall supply complete services in terms of WAF which includes implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.
4	The bidder shall be responsible for replacing and upgrading the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the bank during the entire contact period. Replacement to be done before due date of the product/service.
5	Return merchandise authorization (RMA) process for replacement of appliance to be completed within 24 hours from reporting time of issue.
6	Ensure signature staging to reduce false positive during new signature updates.
7	Ensure real-time signature updates
8	The proposed solution shall not be "single point of failure"; the failure of one or more components of the solution shall not affect the organizational functionality in any way i.e. if WAF is not available, Web application shall not get impacted in any way.
9	The proposed WAF at DRDC shall perform real-time learning policy and configuration sync with existing production devices.
10	Ensure all existing policies, learnings and device configuration of each application migrate to new proposed devices for implementation in all three existing data centres (PDC, ODC, DRDC).

Encrypted traffic Management (SSL Orchestration)

The Scope of work for SSL Orchestration solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to proposed SSL Orchestration (SSLO).

S. No	Scope
1	The Proposed SSL Intercept Solution shall have the ability to transmit decrypted traffic to (in-line) security devices like IPS, NGFW, WAF etc. and re-encrypt traffic after security device inspection.
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	Bidder shall supply complete services in terms of SSLO which includes implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.
4	The bidder would be responsible for replacing and upgrading the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the bank during the entire contact period. Replacement to be done before due of date of the product/service.
5	Return merchandise authorization (RMA) process for replacement of appliance to be completed within 24 hours from reporting time of issue.
6	This solution shall support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure.
7	Review of configured policies, traffic forwarding issues and setup new policies and suggest improvements.

Anti-DDOS

The Scope of work for anti-DDOS solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contract related to or connected to anti-DDOS solutions.

S. No	Scope

1	Design, validate, implement & periodically perform OEM review of anti-DDOS solution (along with all the required solution as per scope of work).
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	24*7*365 monitoring & management aspects of anti-DDOS services.
4	Identify information security threats/ vectors targeting Bank ‘s environment and prevent impact or breach by implementing adequate controls on DDOS appliance to address all kind of DDOS attack.
5	Return merchandise authorization (RMA) process for replacement of appliance to be completed within 24 hours from reporting time of issue.
6	Bidder to ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the identified locations by Bank), enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, backups, audits, support for the proposed hardware/software required for delivering the managed Security Support services.
7	Bidder shall propose solution that shall be capable of retrieving the archived logs for analysis, correlation, reporting and forensic purposes.
8	Bidder shall ensure that for each security incidents, solution shall provide real time remediation guidance.
9	Aid Bank if needed during cyber security drills / audits as and when conducted.
10	Bidder shall develop a Standard Operating Procedure (SOP) for alert management, incident management, forensics, report management, log storage and archiving, Business Continuity. SOP shall also cover log monitoring tool management including configuration, agent deployments, backup, and recovery.
11	Bidder shall provide knowledge transfer and training on the technology, functionality and operations of the anti-DDOS solution to current service integrator and Bank officials.
12	In case of any incident, bidder shall identify the root cause of the attack & suggest preventive measures to avoid facing similar type of attacks again.

Global Server Load Balancer (GSLB) & DNS Security

The Scope of work for GSLB solution includes design, supply, configuration, implementation, integrations, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to GSLB solutions.

S. No	Scope
1	Design, validate, implement & periodically perform OEM review of GSLB solution (along with all the required solution as per scope of work).
2	OEM shall be responsible to provide the future Data Centre Solution Design Document (SDD) consisting of High-Level Design (HLD) and Low-Level Design (LLD)
3	Return merchandise authorization (RMA) process for replacement of appliance to be completed within 24 hours from reporting time of issue.
4	Bidder to ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the identified locations by Bank), enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, backups, audits, support for the proposed hardware/software required for delivering the managed Security Support services.
5	Bidder shall develop a Standard Operating Procedure (SOP) for alert management, incident management, report management, log storage and archiving, Business Continuity. SOP shall also cover log monitoring tool management including configuration, backup, and recovery.
6	Bidder shall provide knowledge transfer and training on the technology, functionality and operations of the GSLB solution to current service integrator and Bank officials.
7	In case of any incident, bidder shall identify the root cause of the attack & suggest preventive measures to avoid facing similar type of attacks again.

Threat Intelligence Feed

The feeds should demonstrate exceptional expertise in delivering high-quality, actionable threat intelligence that enables proactive threat detection and response by integrating this intelligence into Bank's existing IT security infrastructure. The comprehensive feeds should provide real-time insights into emerging threats, vulnerabilities, and adversary tactics, techniques, and procedures (TTPs). Bank is already using the Threat Intelligence services and is willing to strengthen its threat intelligence suite with other feeds.

The scope of work for the successful implementation of the Threat Intelligence Feed solution should include the following:

- The selected bidder shall implement all the three Threat Intelligence Feed solutions in full compliance with the technical and functional specifications outlined in this RFP. The complete solution must be made operational and go live within four (4) weeks from the date of issuance of the Purchase Order (PO).

- As it is the evolving technology, any future evolutionary features enhancing threat intelligence feeds shall be made available to the Bank as a part of the this agreement.

- The bidder shall be solely responsible for provisioning all components necessary for implementation, including but not limited to the solution platform, services, software licenses, APIs, integration mechanisms, and any other tools or utilities required for the effective functioning of the Threat Intelligence Feed solution.

- The bidder must submit a comprehensive Plan of Action (PoA) outlining the methodology, intended use, integration points, operationalization process, and utilization strategy for the Threat Intelligence Feed tailored to the Bank's cybersecurity framework.

- The bidder shall be the single point of contact for all technical assistance and ongoing support. They will be responsible for ensuring the agreed-upon availability and uptime of the solution, including proactive monitoring, incident resolution, and performance tuning.

- The bidder shall be responsible for ensuring comprehensive and detailed training is provided by the Original Equipment Manufacturer (OEM).

5.1.5 RACI – Scope of Implementation (For both Bidder and OEM)

Below Table depicts desired RACI (Responsible-R, Accountable-A, Consulted- C, Informed-I) matrix for proposed engagement which is non-exhaustive. The SI shall submit comprehensive RACI for proposed services in a similar way in their response to RFP.

S. No.	Activity	SI	OEM	RBI
1	Plan, Design, Implementation	R, A	R, A	C, I

S. No.	Activity	SI	OEM	RBI
2	Device Monitoring Best Practices Audit- Identify existing monitoring parameters, recommended monitoring practices, and formulate a corrective action plan.	A	R	C, I
3	Device Health check and Performance Monitoring	R, A	C	I
4	Monitoring Tool/Solutions /Software availability and Support	R, A	C	C, I
5	Service Request Handling	R, A	C	I
6	Incident Detection and Notification	R, A	C	I
7	Incident Troubleshooting	R, A	R	C, I
8	Incident Closure- Restoration	R, A	R	C, I
9	Problem Management- Root Cause Analysis (24 hours)	R, A	R	C, I
10	Configuration Change Plan	R, A	C	I
11	Impact Analysis and Change Validation	R, C	C	I
12	Change Approval	I	C	A, R
13	Change- Method of Procedure	C, I	C	R, A
14	Change Execution	R, A	C	C, I
15	Change Communication	R, A	C	I
16	Impact analysis of use cases, CRF For IT Security solutions	R, A	C	I
17	Software Implementation	R, A	A	C, I
18	Software Security Vulnerability Assessment	R, A	R, A	C, I
19	Configuration Audit, Best Practices	R, A	R, A	C, I
20	Configuration Remediation	R, A	C	C, I

S. No.	Activity	SI	OEM	RBI
21	Capacity Audit and Benchmarking	A	R	C, I
22	Performance Audit	R, A	R	C, I
23	Capacity and Performance Monitoring	R, A	C	I
24	Inventory Management	R, A	C	I
25	License Management	R, A	C	I
26	Reporting	R, A	C	I
27	SLA Performance	R, A	C	C, I
28	SLA Reporting	R, A	C	C, I
29	Service Delivery Review and Governance	R, A	C	C, I
30	First Information report (FIR) on incident (4hrs), Zero Day/ Vulnerability Report	R, A	R, A	C, I
31	Business Continuity Management	R, A	I	C, I
32	Proactive Threat Assessment	R, A	I	C, I

6. Facilities Management Services (FMS)

6.1 FMS

The bidder shall provide on-site Facilities Management Support (FMS) for the solution procured through this RFP at Data Centres starting from the date of issuance of the 'Acceptance Certificate' by the RBI to the Bidder post completion of implementation.

The bidder and OEM engaged through the bidder shall be responsible to ensure that on-site FMS Team deliver the following Operational activities to the satisfaction of RBI.

Bidder shall provide following services under Facility Management Services (FMS):

6.1.1 Device and Performance Monitoring

- Perform daily health checks of the solution components for proper functioning and performance.
- Monitoring the security of the solution on a 24*7 basis. The security events related to the solution need to be monitored for any anomalous or unauthorized activity through the centralized dashboard.
- Utilizing the solution's centralized management console for monitoring and observing related events/logs and alarms and perform first-level action while alerting the relevant teams in parallel viz. ISOC.
- Utilize existing monitoring systems deployed at RBI for monitoring and observing any security-related events/logs and alarms and work towards suitably addressing/remediating the same.
- Uptime reports, device availability and reachability reports
- Threshold monitoring of bandwidth, CPU and memory utilization and reporting of the same to the Bank's official via mail or SMS immediately in case of exceeding the threshold limit
- All relevant reports required for calculation of SLAs

6.1.2 Configuration and Change Management

- Hardware and software maintenance of the proposed solution, Configuration management, Change and release management, audit, and reporting.
- **Device Onboarding**. A Single Change Request Form (CRF) template shall be maintained for device onboarding (As per standard format). The CRF shall be processed only after due approval from the authorized official as per the governance matrix. The records of the CRF shall be maintained permanently.
- The FMS team shall be responsible for ensuring that the solutions/ devices newly introduced in the Bank's environment are configured for integration/ on-boarding with the relevant tool.
- The FMS team shall verify that the new device is on-boarded in the Central Management Console of respective tool(s) for visibility
- Ensuring that the devices newly introduced in the Bank's environment are configured as per OEM recommendations and visible on the Central Management Console.
- Plan configuration change, perform impact analysis, prepare method of procedure and execute changes during approved maintenance window.
- Business Continuity Planning (BCP) including Disaster Recovery
- Periodic summary of changes undertaken including major changes like configuration changes, patch upgrades, etc. and any other minor changes

6.1.3 Capacity, License and Performance Management

- Conduct capacity or utilization audit of hardware capacity and software licenses as per benchmarks prescribed by RBI, and periodically report the same at least once every year. In the event of any device or network segment which is not operating within defined thresholds, OEM shall make a suitable recommendation to ensure RBI does not encounter any incident due to exceeding utilization thresholds.
- Perform daily reporting of key events or statistics from the central management console.
- Ensuring that any software security vulnerabilities identified by the OEM on the solution equipment installed at RBI Infrastructure are properly addressed and providing an annual report from the OEM confirming this. After the total solution is commissioned, the FMS shall be responsible for the overall management and monitoring of the project, as well as coordinating the delivery and installation of hardware and software licenses within the specified time frame.
- Server Security Management and Optimization
- Configuration Backups
- Data Backup & Recovery

6.1.4 Service Request Management

- Handle any miscellaneous operational tasks like managing and updating relevant documentation (like facilitating any required authorization for RMA, performing device configuration backup, etc).

6.1.5 Incident and Problem Management

- End-to-End responsibility for Incident Handling, Incident Detection, Incident Notification, Incident escalation, Periodic Communication, Incident Closure, Update knowledge basis, incident resolution, and Root cause analysis.
- Incident management (problem identification, diagnosis, root cause analysis, and resolution/escalation).
- The FMS Team shall serve as a Single Point of Contact (SPOC) for all incidents and service requests at all the sites related to deployed solution.

6.1.6 Software Release Management

Conduct a proactive risk assessment to evaluate most suitable available software for tools deployed across the Banks' locations as per historic incidents, security vulnerability compliance, running configurations and features deployed. Plan and manage software upgrades for all tools. This exercise shall be done at least once in a year and OEM, in coordination with bidder, is responsible for informing any critical defects or security vulnerabilities that are notified for equipment/ software deployed in RBI network.

Bidder shall ensure that any stable patches/ versions of software/ hardware released by the respective OEMs and as decided as N/N-1 as per bank's policy shall be supported by underlying hardware in terms of capacity, utilisation, performance etc. and if the underlying hardware needs upgrade for the above reason, the same shall be done without any additional cost to the Bank

6.1.7 FMS – Role and Structure

The bidder shall provide the on-site FMS resources as per the distribution structure provided below. On-site FMS services team shall meet the technology skill set requirements as per below.

Indicative Summary of Resources

Team	Availability
L1 Team - Bidder • Continuous monitoring of security solutions and systems. • Immediate response to alerts and incidents. • Documentation of incidents and resolutions. • Initial incident assessment and triage. • Basic issue resolution or escalation to L2/L3 as needed. • User support and troubleshooting. • Logging and tracking of incidents in the ticketing system. Provide on field support (Hands and Feet support). • Install application patches and signed software updates in order to improve performance, enable additional functionality or enhance security standard including but not limited to Performing Scans, Management of the system, Updating of plugins and patches, etc. • To maintain the inventory of entire assets of Cyber Security solutions as per scope of this RFP and maintain and update a database with respect to OS, Database, Web-servers, Application details, IP addresses pertaining to all Security Solutions under scope of this RFP. • Maintain IP addressing schemes, routing information, routing tables, etc. for the Firewall operation.	**24X7 Onsite**
L2 Team – Bidder	**24x7**

• In-depth technical troubleshooting and issue resolution. • Implementation, Management and Monitoring all cyber security Solutions/ Devices/ Components. • Deployment and Installation of all in scope solutions and their monitoring • Implementation of service improvements. • Collaboration with L3 for complex issues. • Regular configuration tasks and change management • Closely monitoring of overall health of the all solutions and submit reports to the Bank with related parameters on a daily basis. • Mitigation and compliance of Information security/cyber security /RBI IT Examination audit points/ VAPT Audit Points/ Internal IS audit Points/ Points pertaining any other internal/external Audit undertaken in the Bank. • Shall maintain the backup of all necessary files including configuration file, in line with Bank's Information security policy /Cyber security policy. Restoration testing process of the backup has to be carried out and recorded on periodic basis all applicable security solutions. • Solutions to be upgraded to recommended levels by OEM immediately on availability of upgrade/patches.	**Onsite**
L3 Technical Lead – OEM Resident Engineer • High-level technical expertise for complex problems. • Design and implementation of advanced solutions. • Performance optimization and capacity planning. • Mentorship and training for L1/L2 teams. • Responsible for timely patch deployment, migration of firmware/ software and deployment of configuration as part of migrated functionality, timely update of necessary signatures, and its functionality after taking complete precaution to avoid outage and downtime. • Maintain network and security architecture diagram and review and update the based-on changes. Further, proper maintenance for LLD and HLD for each solution and regular update of the same. • Provide the suggestions for any enhancements/changes that can enhance the security posture and/or add business value to the delivery framework.	**8X5** **Onsite**
Operations Manager – Bidder • Oversight of daily service operations. • Team management and performance tracking. • Incident and SLA management. • Process improvement and resource allocation.	**8X5** **Onsite**

• Shall develop complete know how of cyber architecture posture of the Bank. Recommendation for Configuration in line with business requirement and industry standard. • Risk assessment and finalizing best possible optimum cyber security architecture design for new Cyber Security Solutions and solutions which are to be upgraded as per scope of this RFP at DC/DR other locations and reviewing of the same. • Aligning the team for DR Drill, Cyber Drill or any other planned/unplanned activities. • Track Hardware AMC Renewal Dates & Validation	

Other requirements

- With respect to devices proposed for current DCs (PDC, ODC, DRDC), facility management services of those devices shall be in accordance with existing network and security architecture, design and policy in these DCs in coordination with FMS & OEM teams currently managing the network and security in these DCs.
- In case of exigencies, L1, L2 and L3 shall be available after business hours and on Sundays and Holidays as well.
- The FMS team shall ensure that adequate man-power is available to meet the deliverables as per the scope of work and maintain performance and availability requirements as per SLA.
- All the relevant documentation including SOPs, workflows, manuals etc. need to be updated by the FMS team in coordination with the bank, OEM & Bidder from time to time.
- Regular training and knowledge updates/ sessions / refreshers shall be imparted by the bidder to the FMS team in coordination with SME from OEM(s) throughout the contract period which shall be reviewed periodically by the bank
- The FMS team shall report the profile, attendance details, key resource and responsibilities and any other details of the team deemed necessary to a SPOC identified at Bank's central site and other locations monthly.
- The Bank reserves the right to periodically review the performance of the bidder/OEM and its employees under the managed services and may ask for replacements if required. The Bank shall increase or decrease the number of resources at any stage if required.
- The successful bidder of the respective project shall mandatorily check background credentials of all the resources with relevant satisfactory report submitted to and accepted by the Bank before any resource to be deployed at any of the Bank's premises. Replacement of resources shall also be deployed after submission and acceptance of the said report.

- The selected bidder shall ensure that proposed team is competent, professional and possess requisite qualifications and experience appropriate to the task they are required to perform under the scope of services and FMS qualifications defined in this RFP.
- If bidder is unable to provide support or any solution component of hardware and software goes end of support during the validity of the contract or upgrade for any of the components is needed for any newly emerged threat/vulnerabilities, then the Bidder shall upgrade the component/ sub-component with an alternative that is acceptable to the Bank at no additional cost to the Bank and without causing any performance degradation and/or project delays.
- As per RBI's requirement, the successful bidder of the project shall be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to RBI.
- The successful bidder of the project shall procure the software license in the name of RBI.
- The proposed solution shall be subjected to Information Technology Audits by the Bank. The successful bidder of the respective project shall provide required support to carry out the audits – pre-launch and post launch - and shall take necessary corrective action to comply with audit observations.
- The bidder shall manage the overall infrastructure comprising of all deployed solutions and the associated infrastructure such that an infrastructure uptime on a quarterly basis, shall be maintained in accordance with Uptime Tier-IV standards of a Data centre.

-

Qualification and Experience requirement

Details of skill set required for the engagement of engineers but not limited to following:

Position	Skill Set
Level-1 (L1)	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP or equivalent of respective OEM with minimum 3 years and above relevant experience ➢ Person shall have adequate knowledge of security devices like Firewalls, SSLO, WAF, DDOS, LB, GSLB and other security devices.
Level-2 (L2) for Firewall/ Anti DDOS	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + OEM Firewall / Anti-DDOS solution with minimum 5 years and above relevant experience.

	➢ Person shall have adequate knowledge of security devices like Firewalls, Anti-DDOS solution. ➢ Shall analyse incidents & identify root cause and act for containment and remediation. ➢ Shall co-ordinate with the different departments/stakeholders for incident analysis and remedial action. ➢ Provides engineering analysis and architectural design of technical solutions. ➢ Knowledge of networking protocols and technologies and network security.
Level-2 (L2) for WAF/ SSLO	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + WAF / SSLO with minimum 5 years and above relevant experience. ➢ Person shall have adequate knowledge of security devices like WAF, SSLO. ➢ Shall analyse incidents & identify root cause and act for containment and remediation. ➢ Shall co-ordinate with the different departments/stakeholders for incident analysis and remedial action. ➢ Provides engineering analysis and architectural design of technical solutions. Knowledge of networking protocols and technologies and network security.
Level-2 (L2) for GSLB/SLB	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + GSLB/SLB with minimum 5 years and above relevant experience. ➢ Person shall have adequate experience of security devices like SLB, GSLB and other security devices. ➢ Shall analyse incidents & identify root cause and act for containment and remediation. ➢ Shall co-ordinate with the different departments/stakeholders for incident analysis and remedial action. ➢ Provides engineering analysis and architectural design of technical solutions. Knowledge of networking protocols and technologies and network security.

Level-3 (L3) for Firewall / Anti DDOS	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + OEM Firewall / Anti-DDOS with minimum 7 years and above relevant experience. ➢ Solution architects are preferred. ➢ Minimum 7 years of experience in handling security related products & services in an organization ➢ Shall analyse incidents independently & identify root cause and act for containment and remediation. ➢ Provides engineering analysis and architectural design of technical solutions. ➢ Sound analytical and troubleshooting skills. ➢ Good Team Management and co-ordination skills
Level-3 (L3) for WAF /SSLO	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + WAF/SSLO with minimum 7 years and above relevant experience. ➢ Solution architects are preferred. ➢ Minimum 7 years of experience in handling security related products & services in an organization ➢ Shall analyse incidents independently & identify root cause and act for containment and remediation. ➢ Provides engineering analysis and architectural design of technical solutions. ➢ Sound analytical and troubleshooting skills. ➢ Good Team Management and co-ordination skills
Level-3 (L3) for SLB/GSLB	➢ BE/BTech/BCA or Master Degree in CS/IT with either certification CEH or CCNA/CCNP + SLB/GSLB with minimum 7 years and above relevant experience. ➢ Solution architects are preferred. ➢ Minimum 7 years of experience in handling security related products & services in an organization ➢ Shall analyse incidents independently & identify root cause and act for containment and remediation. ➢ Provides engineering analysis and architectural design of technical solutions. ➢ Sound analytical and troubleshooting skills. Good Team Management and co-ordination skills

Project Manager	➢ B.E. /B.Tech in Computer Science/Electronics/IT/Electrical Engineering/ MCA/MBA. ➢ At least one Security certifications PMP/ITIL expert/CISA/CISM/CISSP. ➢ Total experience of minimum 15 years and above out of which minimum 8 years of experience in handling security related products & services in an organization of repute. ➢ Minimum experience of 3 years as L3 level. ➢ Person shall have adequate knowledge of Firewall, NIPS, WAF, Anti-DDoS and other security devices/solutions. ➢ Overall knowledge/experience of Architectural Design and Best practices on Network and Cyber Security. ➢ Excellent Team Management, co-ordination and communication skills ➢ Co-ordinate with company to get HR details like BGV, EPF Challans, etc ➢ Ensure that FM resources are deployed properly, and all shifts have adequate resources.

6.2.7.1 Direct Premium Support with respective OEMs for all the IT security solutions procured under this RFP:

Bidder shall maintain all the IT Security solutions and its related components, procured under this RFP, under TAC direct premium support on 24x7x365 basis from the respective OEMs throughout the period of the contract with the Bank.

Bidder has to quote for highest/ premium support available from the respective OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features etc. for all those OEMs.

7 Bidder's Eligibility Criteria

S. No.	Eligibility Criteria	Documentation Required
1.	The Bidder should be a Registered Indian Entity under the relevant statutory provision and should have been in business for at least last five years as on date of issue of this RFP.	Attested copy of the Certificate of Incorporation / Registration of the Bidder
2.	The bidding entity should have minimum average annual turnover of ₹ 970 Crore (Rupees Nine-Hundred Seventy crore) and a positive net worth in each of the last three financial years (i.e., FY2021-22, FY2022-23 and FY 2023-24).	Audited financial statements of the bidding entity indicating the annual net worth and turnover as set forth in the eligibility criteria and summary of annual

		turnover and net worth certified by Chartered Accountant OR Statutory Auditor Certificate
3.	1. The Bidder should have experience of supply/implementation/maintenance of Project(s) of similar nature[$] in BFSI/Govt sector in India in the last five years (Either the date of Purchase Order or sign-off document should be within last 5 year from the date of issue of this RFP). Out of such projects: a) Minimum One Project costing not less than ₹ 155,00,00,000/- (Rupees One hundred and Fifty-Five Crore only) OR b) Minimum Two projects costing not less than ₹ 97,00,00,000/- (Rupees Ninety-Seven Crore only) each. OR c) Minimum Three projects costing not less than ₹78,00,00,000/- (Rupees Seventy-Eight Crore only) each. AND 2. Experience of supply / implementation / maintenance of atleast one project in BFSI sector in India with project cost not less than ₹78,00,00,000/- (Rupees Seventy-Eight Crore only). The total project value mentioned is inclusive of taxes. Further, multiple purchase orders for same client and similar nature within the time frame mentioned will be considered. **$Similar Nature**: Project of similar nature means supply/implementation and maintenance/ FMS of security solutions such as Security Operations Center/External and Internal Firewall/Web Application Firewall/Load Balancer (LB)/Global Server Load Balancer (GSLB)/anti-DDOS/ Threat Intelligence Feeds, etc.	The Purchase Order + Project completion/ commencement (for ongoing projects) certificate/relevant document from the client

4.	The bidder should have authorisation from the OEM to quote their products and should be authorised business and service partner of the OEM for all proposed tools. It should ensure Service support till the Validity of the project.	Manufacturers Authorization Letter/Form (MAF) from OEM in favour of Bidder must be enclosed

8 Evaluation Process of Bid

Evaluation Methodology

8.1. The objective of the evaluation process is to evaluate the bids to select an effective and best fit solution at a competitive price. The evaluation will be undertaken under the guidance of the Technical Advisory Group (TAG) formed by the Bank which comprises of Bank officials and external experts. The decision of the TAG shall be final and binding.

8.2. RBI will follow three-stage evaluation and selection process:

Stage I - Eligibility: The documents submitted by Bidders in support of Eligibility Criteria will be opened and evaluated in Stage I. Bidders who do not meet the prescribed eligibility criteria will not be considered for Technical Evaluation.

Stage II – Technical Evaluation: The documents submitted by Bidders in support of Technical Evaluation will be opened and evaluated in Stage II.

Stage III - Commercial Bids Evaluation: Commercial bids of only Technically Qualified bidders in Stage II will be opened in the third stage**.**

Documents evaluated at various stages are mentioned at para 23 (Bidding process).

8.3. The 'Technical Bid' will contain the exhaustive and comprehensive technical details, whereas the 'Commercial Bid' will contain the pricing information. The Technical Bid shall **NOT** contain any pricing or commercial information at all and if the Technical Bid contains any price related information, then that Technical Bid would be disqualified and would **NOT** be processed further.

8.4. Bids shall be assessed in accordance with **Quality Cost-based Selection(QCBS)** method wherein 60 percent weightage will be given to the scores obtained after evaluation of technical proposal and 40 percent weightage will be given to commercial proposal. The highest ranked bidder

based on cumulative technical and commercial evaluation ranking will be considered as selected bidder.

Technical Bid	Commercial Bid	Overall Score
60	40	100

DETAILED MARKING SCHEME FOR TECHNICAL EVALUATION

8.5. Functional and Technical requirement are categorized into following two types:

i. Mandatory [M]: These requirements are those which are absolutely essential for the functioning of the complete solution and are to be met in their entirety in the precise manner as documented in the requirements for respective products in this document. If bidder does not meet mandatory requirements, their bid will not be considered for further evaluation and they will disqualify at technical evaluation stage and not be eligible for next stage of evaluation i.e., Commercial Evaluation.

ii. Desirable Functional Requirement [D]: These requirements are good to have for enhanced efficiency and effectiveness of the overall solution but not mandatory. Bidder is required to meet at least 60% of the total desirable functionality of each and every solution component specified in **Annex III** (Technical Specifications).

8.1 Technical Bid Evaluation Criteria

Technical Qualification (Submission of all the relevant annexes as part of RFP)	Strength/Capability of the Proposed solution shall be assessed in terms of compliance to mandatory and desired feature which comprises of functional Specifications. * The Combined score will be calculated up to three decimal places. * Bidder is required to meet at-least 60% of the total desirable functionality of every solution component i.e. bidder has to score minimum 60% marks in	**Categories:** A - Internal FW (7 marks) B - External FW (7 marks) C - FW SandBox APT D - WAF (7 marks) E - Load Balancer (7 marks) F - SSLO (7 marks) G - GSLB (6 marks) H - Anti-DDOS (6 marks) I – Three different Threat Intelligence Feeds (TIF) (3 marks – 1 mark for each TIF)	**50**

	each of the categories listed in next column except category C which is mandatory. Note : Individual solutions will be assigned marks out of 100 as per Annex III. These marks will be normalised as mentioned above for each solution.		
Bidder experience in Supply/implementation/Maintenance of the similar solution in the last five years (either Purchase order date or sign-off date should be in last five years) (supported by necessary documentary evidence)			**30**
	Experience of implementation/ maintenance of proposed tools in single organization in Govt./BFSI sector in India with project cost of at least 50 crores (Inclusive of taxes): • atleast 5 products out of IFW/EFW/WAF/SSLO/anti-DDoS/SLBs/GSLBs/TI Feeds - 8 marks • atleast 4 products out of IFW/EFW/WAF/SSLO/anti-DDoS/SLBs/GSLBs/TI Feeds - 6 marks • atleast 3 products out of IFW/EFW/WAF/SSLO/anti-DDoS/SLBs/GSLBs/TI Feeds - 4 marks The project should be signed off in the last Five (05) years from the date of the RFP.	The Purchase Order + Project completion/Sign-off document from the client	**8**
	ii) Experience of supply/implementation /maintenance of project of similar nature (as defined in eligibility criteria) in **BFSI** sector in India with project cost of:	The Purchase Order + Project completion/ commencement (for ongoing projects) certificate from the client	**10**

	• At least 200 crores - 10 marks • At least 150 crores - 8 marks • At least 100 crores - 6 marks • At least 50 crores - 4 marks The total project value mentioned is inclusive of taxes.		
	iii) Experience of implementation / maintenance of proposed OEM solution for Perimeter and Internal Firewall in Govt./BFSI sector in India by the Bidder • Implementation of both external and internal firewall in atleast two (02) organisation - 4 marks • Implementation of both external and internal firewall in atleast one (01) organisation - 2 marks • Implementation of either external or internal firewall in atleast one (01) organisation - 1 mark	The Purchase Order + Project completion/ commencement (for ongoing projects) certificate from the client	**4**
	iv) Experience of implementation / maintenance of proposed OEM solution for SSL Orchestrator/DDOS solution in Govt./BFSI sector in India by the Bidder in * atleast two (02) organisation - 4 marks * atleast one (01) organisation - 2 marks	The Purchase Order + Project completion/ commencement (for ongoing projects) certificate from the client	**4**
	v) Experience of implementation / maintenance of proposed OEM solution for	The Purchase Order + Project completion/ commencement (for	**4**

	Web Application Firewall (WAF) in Govt./BFSI sector in India by the Bidder. • Yes - 4 marks • No - 0 mark	ongoing projects) certificate from the client	
Presentation for evaluation criteria	Qualitative assessment based on Demonstration of understanding of the Bank's requirements through providing: ➢ Understanding of the objectives of the project: The extent to which the Bidder's approach and work plan respond to the objectives indicated in the Statement/Scope of Work ➢ Ease of migration ➢ Ease of implementation ➢ Synergy with existing Infrastructure ➢ Risk Mitigation Strategy ➢ Incident response and remediation ➢ Coherence with project plan and approach document ➢ Unique implementation features, value addition through innovation, automation or improved practices/process etc. ➢ Accelerate project Implementation timelines without compromising on quality.		**20**

8.6. The eligible bidders after Stage I evaluation, would be invited to RBI to make a presentation (after opening of technical bid) detailing the proposed

infrastructure, implementation approach, rollout strategy, facility management services for the solution which would be evaluated based on the following:

i. The bidder(s) would be required to present details of the requirements as mentioned elsewhere in the RFP and have to specify how they are meeting the requirements for the solution.
ii. The bidder(s) would be required to present details of the proposed hardware and its related environment, configuration etc.
iii. The bidder(s) may be required to present details of the approach & rollout strategy.
iv. The bidder should detail on the licensing model/scalability/ dependency on appliance and any other factor relevant for the various components of the total solution wherever applicable.
v. The bidder should conform to all the functional requirements and technical specifications for each of the components as mentioned in the RFP.
vi. Any dependencies/risks/assumptions with proper justification should be explicitly called out as part of the presentation.
vii. The bidder(s) would be required to present details of the post implementation support including alignment of FMS for each Data Centre of the Bank.
viii. Plan and processes to support the requirement of system uptime of 99.9%.

8.7. The bidder should envision and present/document the risks associated if any for the implementation and successful rollout of the solution and corresponding risk mitigation strategies.

8.8. The bidder is expected to provide, as a part of the technical bid, a detailed document that explains the approach and methodology proposed by the bidder for the implementation of the proposed solution including facility management services of the solution.

8.9. The Bidder should provide explanation on the implementation and facility management process that is proposed for the Bank including details and experience of how the same was utilised and applied in similar projects implemented elsewhere by the bidder.

8.10. The Bidder should note that it is mandatory to score an overall cut-off score, which is at least 70 marks of the total 100 marks allocated for the technical

evaluation. Further, the bidder should also score at least overall 60% of marks in each of three sections i.e., Technical Specifications, Implementation Experience and Presentation. The Bank shall disqualify any Bidder who does not achieve the cut-off on the above-mentioned bidding parameters from the bidding process.

8.11. The Bidder with the highest technical score shall be declared as T1.

8.12. The technical scores of the qualifying bidders shall not be disclosed to all the bidders.

Disqualification Parameters in Technical Bid Evaluation

8.13. The Bank at its discretion may reject the proposal of the Bidder without giving any reason whatsoever, if in the Bank's opinion, the Solution sizing was not made appropriately to meet the performance criteria as stipulated by the Bank.

8.14. The Bank at its discretion may reject the proposal of the Bidder without giving any reason whatsoever, if in the Bank's opinion, the Bidder could not present or demonstrate the proposed solution as described in the proposal.

8.15. The Bank at its discretion may reject the proposal of the Bidder in case the responses received from the reference sites are negative.

8.16. The bidders who do not qualify in the Eligibility criteria and who do not adhere to the integrity pact will be disqualified.

8.17. The Bank reserves the right to disqualify any bidder, who is involved in any form of lobbying/ influencing/ canvassing etc., in the evaluation / selection process

8.18. And any other disqualification criteria mentioned in this RFP.

Commercial Bid Evaluation

8.19. Commercial bids of only those eligible bidders who qualify in the technical evaluation shall be opened. Commercial bids of the other bidders shall not be opened.

8.20. Bidders will have to submit the Commercial bid in the format **Annex VI.** Bank shall upload the price bid form in Excel format on MSTC portal. The bidder is expected to submit the Commercial bid **exclusive of GST.** All the applicable taxes should be calculated on the base price and indicated separately.

8.21. Commercial Bid shall contain the prices for all the items indicated in the Technical BoM (without price) including any additional items proposed by the bidder.

8.22. Bank may call for any clarifications/additional particulars required, if any, on the technical/ commercial bids submitted. The bidder must submit the clarifications/ additional particulars in writing within the specified date and time. The bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time.

8.23. The TCO for the purpose of commercial evaluation shall be arrived by calculating:

TCO

Sr No	Description	Total
1	One time Cost of Hardware + Software with 3 Years Warranty and Support and Implementation	
2	AMC/ ATS of the Proposed Solution for Year 4 and Year 5	
3	Facility Management from Year 1 to Year 5 and Other Services Cost	
	Total Cost of Ownership (TCO) in INR for 5 Years = (1+2+3)	

8.24. The payments shall be done as per the payment terms and milestones (para 14).

8.25. The Prices of the passive components and labour charges will be fixed for a minimum period of one year from issue of PO and for all subsequent years the new amount will be arrived based on the indexation formula as given in RFP.

8.26. Bidder has to provide quote for different type of human resources under the Facilities Management services for 1st year only and cost for year 2 to 5 will be calculated with 5% escalation. Accordingly, Total FMS cost for the contract period will be derived for TCO calculation.

Techno-commercial Score

8.27. Technical Evaluation will carry 60% weight while Commercial Bid will carry 40% weight for arriving at Technical high (T1) and Lowest cost (L1) ranking. The composite techno-commercial score shall be calculated as follows:

Total Score = {(L1 price / C)*0.4 + (T / T1 score) *0.6}x100

Where:

C: Commercial bid of the respective bidder

T: Technical score of the respective bidder

L1: Lowest price amongst all qualified bidders

T1: Highest Technical score amongst all qualified bidders

The Composite score will be approximated (to nearest whole value) up *to two decimal places.*

8.28. Bidder with the highest Techno-commercial Score would be awarded the contract. In case of a tie of Techno-commercial Score between two or more Bidders, the Bid with higher technical score would be chosen as the successful bidder

8.29. RBI will notify the name of the Successful Bidder only.

9 Awarding Methodology

Through this RFP, the Bank intends to procure the following items:

a) Hardware and Software Components with three-year warranty and implementation;
b) Annual Maintenance Contract (AMC)/Annual Technical Support (ATS) for Year 4 and 5;
c) Facility Management Services (FMS) and services for Year 1 to Year 5;

In the event of significant deviations in the prices quoted by different bidders for items (a) to (c), the Bank reserves the right to select separate bidders for each category. Selection will be based on the lowest cost quoted for each line item, after applying the Techno-Commercial evaluation formula specified in Paragraph 8.27.

10 Delivery Schedule

10.1 The Bank would like to have the following schedule for completion of the activities from the date of placement of orders for proposed solutions

Sr. No.	Deliverables	Completion
1	Signing of Contract/Agreement with the Bank	Within 45 working days from the date of Purchase order
2	Delivery of all items (as per Purchase Order) at designated sites of the Bank	Within 8 weeks from the date of Purchase order
	Site Survey, HLD LLD Implementation planning, etc. may start after the issue of purchase order for faster implementation.	

3	Implementation of the proposed solutions & completion of User Acceptance test, Satisfactory completion of Audit, Validation & Certification by all OEM/s for respective components and performance of the Solution.	Within 36 weeks from the date of Purchase order
4	Project Sign-off (Go-Live)	Completion of point no. 3 and deployment of FMS resources

Delivery Timelines for Threat Intelligence Feeds

Sr. No.	Deliverables	Completion
1	Delivery of licenses	Within 2 weeks from the date of Purchase order
2	Implementation of the proposed solutions & completion of User Acceptance test.	Within 4 weeks from the date of Purchase order
3	Project Sign-off (Go-Live)	Completion of Point 1 and 2

10.2 The Hardware, software and associated documentation so received shall be in good working condition at the designated locations of the Bank.

10.3 The delivery of the solution shall be deemed complete when an authorised representative of the Bank issues certification for Material Delivery Completion of the proposed solutions at their respective sites.

10.4 The bidder shall communicate the timelines for the Installation schedule and any other relevant details to the Bank as part of its project plan.

10.5 The installation shall be deemed to be complete after successful completion of Acceptance Test.

10.6 The Bidder shall resolve any system software and integration issues with existing systems and application related problems during installation of the proposed solution.

10.7 During Acceptance Test of the proposed solution, if the solution is found to be not meeting the required specification and performance expectations, the Vendor shall take remedial measures including up-gradation of the proposed solution or any of component there under, including replacement thereof, at no additional cost

to the RBI, to ensure that the proposed solution meets the requirements of RBI as envisaged in this RFP.

10.8 The bidder is required to ensure that OEM/s services team conducts an audit of implemented solution and validate / confirm that implementation and configuration has been done as per OEM's best practices and the design is suitable to deliver 99.9% uptime, and thereafter issue the Certificate signed by the Authorised signatory, which would be considered as final user acceptance test i.e. Stabilisation of the Project.

11 Site Particulars

Non-familiarity with the site conditions might not be considered a reason either for extra claims or for not carrying out the work in strict conformity with the timelines and specifications. Successful bidder is expected to familiarise themselves with the site conditions and operationalise the proposed solution as per the timelines in the proposed delivery schedule in this RFP.

12 Service Level Agreement (SLA)

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be expected from the selected OEM/SI during the implementation of each proposed solution / project.

Implementation SLA

S. No.	Service Category	Target	Penalty
1	Delivery of all items (as per Purchase Order) at designated sites of the Bank	8 weeks from the date of Issue of Purchase Order	Penalties will be applicable after 8 weeks, if the Delivery is not completed and the delay is solely attributable to vendor. Penalty for late delivery at 0.5 (half) % of the undelivered portion of order value exclusive of taxes per week will be charged for every week's delay beyond 8 weeks subject to a maximum of 10% of the purchase order value exclusive of taxes. Penalty will be calculated on per week basis.

2	Sign-off of the proposed solution	36 weeks from the date of Issue of Purchase Order	Penalties will be applicable after 36 weeks, if the installation and operationalization and Audit, Validation & Certification by all OEM/s for respective components and performance of the Solution is not completed and the delay is solely attributable to vendor. A penalty of 0.5 (half) % of the implementation cost exclusive of taxes per week subject to a maximum of 10% of the Purchase Order Value exclusive of taxes.

Facility Management Service

The definitions and terms for SLA in the Contract for following terms shall have the meanings as set forth below:

I. Service Levels are calculated based on the "Business Utility" of the solution where:

a. Business Utility (BU) is calculated in percentage as

$$BU\ (\%) = \frac{B_{OH} - B_{DT}}{B_{OH}} * 100$$

Where B_{OH}= Business Operation Hours and B_{DT}= Business Downtime.

II. "Business Operation Hours" for the Bank would be 24x7x365 minus the planned downtime which can be taken only with prior notice to Bank and with mutual consent of Bank and the bidder.

III. "Business Downtime" is the actual duration for which the proposed solution is not able to service the Bank, due to failure of solution or any component of infrastructure thereof, as defined by Bank in the RFP and thereafter in the Contract and agreed by the Bidder. The "Business Downtime" would be calculated on monthly basis for all parameters for performance appraisals and the downtime would form part of core measurement for assessment/ escalation/ penalty, etc.

IV. The severity would be as follows. However, it will be Bank's discretion to assign/alter the severity parameter of the incident appropriately.

a. Critical: In case multiple subsystems are down threatening business continuity and multiple users are affected, it shall be considered as a Critical incident.
b. High: In case any of the subsystem is down causing high impact on business operations and few clients are affected, it shall be considered as a High Severity incident.
c. Medium: In case an essential functionality of the Total Solution becomes unavailable which is not actually hampering the business but may impact few services if not attended immediately shall be termed as medium.
d. Low: The incidents would be termed as low, which does not have any significant impact on the business or functionality e.g:

i. A minor problem or question that does not affect the business operations,
ii. An error in software product Documentation that has no significant effect on operations; or
iii. A suggestion for new features or enhancement.

Severity of Incident	**Resolution time (T)**	**Penalty**
Critical	T = 1 hrs from the time of incident	No Penalty.
	T1 = T+2 hours, and if the resolution time is between T and T1	2% of the Quarterly Amount payable, for every unresolved call.
	T2 = T1+2, and if the resolution time is between T1 and T2	3% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable.
	> T2	5% of the Quarterly Amount payable for every unresolved call, up to 10% of Quarterly Amount payable.
	No of incidents in a quarter > 2	5% of the Quarterly Amount payable for every incident, up to

		10% of Quarterly Amount payable.
High	T3 = T + 0.5 hrs	No Penalty
	T4 = T3 + 2.5 hrs, and if the resolution time is between T3 and T4	2% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable
	T5 = T4+ 2.5 hrs, and If the resolution time is between T5 and T4	3% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable
	> T5	5% of the Quarterly Amount payable for every unresolved call, up to 10% of Quarterly Amount payable
	No of incidents in a quarter > 3	5% of the Quarterly Amount payable for every incident, up to 10% of Quarterly Amount payable
Medium	≤ 2 hours from time of incident logged.	No Penalty
	> 2 Hours and ≤ 4 Hours	2% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable
	> 4 Hours	3% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable
	No of incidents in a quarter > 5	5% of the Quarterly Amount payable for every incident, up to 10% of Quarterly Amount payable
Low	1 day from the time of incident logged at the help desk	No penalty
	> 1 day and ≤ 10 days	2% of the Quarterly Amount payable, for every unresolved

		call, up to 10% of Quarterly Amount payable.
	> 10 days	3% of the Quarterly Amount payable, for every unresolved call, up to 10% of Quarterly Amount payable
	No of incidents in a quarter > 10	5% of the Quarterly Amount payable for every incident, up to 10% of Quarterly Amount payable

Note: The response time for all Types of Help Desk services incidents shall be within 15 min.

Overall Availability Target SLA of **99.9%** will be calculated as per below formula:

Total Solution Uptime – Total Qualifying Outage Time

= ---------- * 100

Total Solution Uptime

- The SLA performance measurement shall be tracked and reported every month, referred to as Reporting Period. However, the penalty calculation for not being able to fulfill SLA will be aligned with quarterly invoicing period, referred to as Measurement Period. The 99.9% uptime translates approximately to 2 hrs 11 mins 29 secs acceptable downtime in a quarter. A penalty of 1% of the Quarterly Amount payable every one hour after the end of above period will be applicable.
- The maximum penalty during a measurement or invoicing period will be capped to 10% of total invoice value for the applicable period.
- First Information Report of any incidents should be communicated to the Bank within 4 hours from the time of occurrence of the incident/issue.
- Root Cause Analysis (RCA) of any incidents should be communicated to the Bank within 24 hours from the time of occurrence of the incident/issue.

Indicative List of issues covered under various service levels

S. No.	Service Area	Service Level – Business Utility	Penalty*
1.	Downtime of standby/ HA components	Alerts within 5 minutes. Response & resolution time of 24 hours.	1% every one hour after end of resolution period of 24 hours within the overall cap.
2.	Report & Dashboard	Periodic reports to be provided as decided by the Bank.	**Daily Reports:** Critical reports should be submitted as and when required. Timings will be mutually decided. Delay in reporting for daily report for more than 1 hour shall incur a penalty of 3% of quarterly charges. **Weekly & Monthly Reports:** To be decided mutually. Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 5% of quarterly charges.
3.	Solution management – Version/ Release/Upgrades / Patches	Bidder to inform RBI team and ensure that entire stack of proposed solutions – firmware, software, middleware, etc. are updated with latest firmware, patches, upgrades, release, version, etc. as per the Bank policy (N-1).	· Penalty of 2% for every fortnight for not informing of the Bank of latest versions / release/upgrades/ patch for all the solutions upon its release. · Penalty of 2% for every week for not informing of critical security patches of all the proposed solution components. · Penalty of 2% for every week of delayed updating/patching beyond mutually agreed upon time schedule for any proposed solution component once notified by the Bank.
4.	Audit of proposed	Proposed solution infrastructure may be	Audit observations to be closed in mutually agreed timeframe.

	solution components	subjected to audit from Bank and/or third party	· Penalty of 5% for each week of delay in implementation of critical and important observations. · Penalty of 1% for each repeated observation. · Cap of 10% of quarterly charges per audit.

**Penalty is percentage of Quarterly charges except for those items where other percentage has been explicitly mentioned.*

13 Overall Liability of the Bidder

The Bidder's aggregate liability in connection with obligations undertaken as a part of this Project 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 excluding taxes.

Notwithstanding anything to the contrary elsewhere contained in this or any other contract between the parties, neither party shall, in any event, be liable for any indirect, special, punitive, exemplary, speculative or consequential damages, including, but not limited to, any loss of use, loss of data, business interruption, and loss of income or profits, irrespective of whether it had an advance notice of the possibility of any such damages.

14 Right to Verification

RBI reserves the right to verify any or all statements made by the Bidder in the tender document and to inspect the Bidder's facilities, if necessary, to establish to its satisfaction about the Bidder's capacity to perform the job. The technical evaluation will be based on such information.

RBI, if deemed fit, will inspect any or all of the equipment at OEM's manufacturing site before shipment to the Bank, to verify that the equipment (s) supplied to RBI are as per the technical specification specified in the tender document or purchase agreement.

15 Payment Terms and Milestones

The payment milestone shall be spread as per the following schedule:

S. No.	Milestones	Payment	Remarks
1	Delivery of hardware and software at designated sites of the Bank for the projects and signing of the contract with RBI	50% of total delivered Hardware & Software Licenses cost	After confirmation of delivery of items and successful Power-On-Self-Test (POST) at respective sites.
2	After Go Live/Sign-off i.e., after acceptance test and audit, validation and certification by all the respective OEM/s at all the sites.	40% of total Hardware and Software Licenses cost and 100% of Implementation cost	After submission of sign-off document from RBI on-site team
3	On completion of 3 years warranty period **OR** against submission of Bank guarantee of equivalent amount covering the contract period	Balance 10 % of Hardware and Software cost	PBG for implementation equivalent to 10% of the Purchase order (PO) value to be submitted within 30 days of the date of PO and will be returned on submission of PBG for maintenance Performance Bank Guarantee (PBG) for maintenance for an amount equivalent to - Annual cost for AMC, FMS and any other recurring charge “or” -10% of the contract value (excluding AMC and FMS) whichever is higher

			PBG will be valid for the contract period for due performance and fulfilment of the contract by the Bidder
4	AMC / ATS and Facility Management Service / Any other services	After end of each Quarter	Quarterly on arrear basis subject to fulfilment of SLA terms and certification from Data Centres for the same
5	Payment towards Cyber Threat Intelligence Feed Subscription Services.	Yearly in advance	Yearly in advance subject to sign-off criteria and certification from Data Centres for the same

*The completion of delivery of licenses should be illustrated through system generated report in the name of RBI/central management dashboard to establish its availability for use by the Bank.

Payment towards Facility Management Services, OEM Services and AMC / ATS for IT Security Infrastructure for Bank's Data Centres

i The amount towards Facilities Management Services and AMC / ATS shall be paid in arrears in equivalent to Quarterly Payments to the System Integrator and will be calculated as illustrated below:

ii Indexation Formula - I to be used for Payment of Facility Management Services Cost from 2nd year onwards.

$A = B \{15 + 85 \times (CPI_c/CPI_p)\} \times 1/100$

Where

A = The Person Month rate for services for the current year.

B = The Person Month rate for services for the previous year.

CPI_c = Consumer Price Index for industrial workers for Mumbai City 6 months prior to the commencement date of contract for the current year

CPI_p = Consumer Price Index for industrial workers for Mumbai City 6 Months prior to the commencement date of contract for the previous year

iii Indexation Formula - II to be used for Payment of AMC / ATS from 5th year onwards is as under:

$A_c = B_p \{15 + 45 \times (WPI_c/WPI_p) + 40 (CPI_c/CPI_p)\} \times 1/100$

Where

A_c = the contract amount for the current year

B_p = the contract amount for the previous year

WPI_c = Wholesale price Index for Electrical Products 6 months prior to the Commencement date of contact for the current year

WPI_p = Wholesale Price Index for Electrical Products 6 months prior to the Commencement date of contact for the previous year

CPI_c = Consumer Price Index for industrial workers for Mumbai City 6 months prior to the commencement date of contract for the current year

CPI_p = Consumer Price Index for industrial workers for Mumbai City 6 Months prior to the commencement date

iv The amount of the Quarterly Payments will be in-line with the SLA parameters as defined in the RFP and the applicable penalties shall be deducted from the Quarterly Payments

v Prices shall be valid for a period of One year from the issue of Purchase Order. The Bank will refer to these prices, when in future it plans to augment the capacity.

16 Earnest Money Deposit

1. Bidder may submit the Earnest Money Deposit (EMD) value in Indian Rupees (INR) through a Bank Guarantee 'only' as per **Annex XVIII.**
2. The value of the EMD is ₹10,98,64,377/- (Rupees Ten Crore Ninety-Eight Lakh Sixty-Four Thousand Three Hundred Seventy Seven only).
3. The EMD/BG should be in favour of Chief General Manager–in–Charge, Department of Information Technology, Central Office, Reserve Bank of India, Mumbai.
4. The EMD/BG should be valid for a period of one year from the last date of submission of bid. The non-submission of EMD/BG will lead to rejection of the bid. The irrevocable BG issued by a scheduled commercial bank only, shall be acceptable to the RBI.
5. The physical copy of Bank Guarantee must be submitted before the technical bid opening.

6. If the EMD is received after the designated date and time for submission of the Bid, the RBI, at its discretion may reject the bid.
7. EMD of unsuccessful Bidders shall be returned within **30 days** from the final result of the bidding process and declaration of the Successful Bidder.
8. No interest shall be payable by the Bank to the Bidders on Earnest Money Deposit for the period it is with the Bank.
9. EMD of the successful bidder will be returned on submission of the Performance Bank Guarantee of **10%** of the purchase order as per relevant Annex "Performance Bank Guarantee Performa".
10. Offers made without the BG for Earnest money deposit will be rejected.
11. The BG of Earnest money would be invoked in the following scenarios:
    a. In case the Bidder withdraws the bid prior to validity period of the bid without providing any satisfactory reason.
    b. In case the successful Bidder fails to accept and sign the contract as specified in this document without any satisfactory reason; or
    c. In case the successful Bidder fails to provide the performance bank guarantee for the amount indicated in the Table for payment terms within 30 working days from the date of purchase order.

17 Performance Bank Guarantee

The successful Bidder, shall at his own expense, submit Performance Bank Guarantee in the name of:

Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001.

Within **Forty-Five Working (45) days** from the date of issue of Purchase Order. Performance Bank Guarantee shall be obtained by the System Integrator from a scheduled commercial bank, payable on demand in terms of relevant Annex for Bank Guarantee format, for an amount equivalent to 10% of the purchase order by the Bidder. This will be valid till the Stabilisation phase and payment associated with this

milestone and submission of PBG for maintenance for release of last payment instalments.

Without prejudice to the other rights of the Purchaser under the Contract in the matter, the proceeds of the performance bank guarantee shall be payable to the Bank as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract.

The Bank shall notify the Bidder, in writing, of the invocation of its right to receive such compensation, indicating the contractual obligation(s) for which the Bidder is in default.

I. The Performance Bank Guarantee may be discharged upon being satisfied that there has been due performance of the obligations of the Bidder under the contract.
II. The Performance Bank Guarantee shall be denominated in Indian Rupees (INR) and shall be valid/ renewed from time to time for the period of contract as per the Terms of payments.

The successful Bidder shall ensure, the Performance Bank Guarantee is valid at all times during the term of the subsequent contract (including any renewal) and for a period of 60 days beyond all contractual obligations.

18 Liquidated Damages

The Bidder should strictly adhere to the implementation schedule, as specified in the RFP or Contract, executed between the Parties for performance of the obligations arising out of RFP terms and any delay attributable to vendor, will enable the purchaser to resort to any of the following.

i The bidder shall be liable to pay the RBI a penalty for reasons solely attributable to the bidder and not the bank, subject to **a maximum of 10%** of the aggregate contract amount exclusive of taxes. Bank reserves its right to recover penalty amount by any mode such as adjusting from any payments to be made by Bank to the Bidder.
ii If any incident occurs during implementation of the project and results in business disruption given the cause for incident is determined to be solely attributable to the Vendor, the Bank reserves the right to impose liquidated damages. The Vendor

will be liable to pay a penalty for each day of business downtime caused, calculated at 1% (one percent) of the total purchase order value per day, subject to a maximum penalty cap of 10% of the purchase order value. The penalty for downtime will be calculated on a 24-hour basis from the time the incident occurred until resolution.

iii Termination of contract fully or partly and claim liquidated damages.

In case of the termination of the purchase order by the RBI due to non-performance of the obligations arising out of the purchase order, the Performance Bank Guarantee will be forfeited.

All disputes of any kind arising out of supply, commissioning, acceptance, maintenance etc., shall be referred by either party (Bank or Bidder) in terms of the para on “Dispute Resolution Mechanism” in this document.

19 Various penalties provisions

(i) Delay in submission of PBG

In case of delays in submission of Performance Bank Guarantee within stipulated time period, penal charges for delay in submission of Performance Bank Guarantee shall be recovered from the bills of the vendors at the extant Bank rate on the entire amount of the Bank Guarantee as prescribed for the number of days of the delay.

In case, PBG for the maintenance has been submitted for a period less than the period of the entire contract and the same has not been renewed and submitted before the expiry of the existing PBG, penal charges for delay in submission of Performance Bank Guarantee shall be recovered from the bills of the vendors at the extant Bank rate on the entire amount of the Bank Guarantee as prescribed for the number of days of the delay.

(ii) Delay in deployment of FMS resources/Non deployment of FMS resources

In case the bidder does not deploy qualified FMS resources as stipulated in this RFP after implementation of the project, penalty equivalent to the one percent of the cost of that specific resource per day will be applicable for the period of the delays. In case of change in any resource due to any reasons, the replacement should be provided

before relieving of the existing resources to ensure knowledge transfer to the new resources. In case of violations of the same, penalty will be applicable as stipulated above.

20 Acceptance Test

After integration and implementation of the proposed solution, the bidder shall be required to perform Acceptance Test and demonstrate all the functionalities required as per this RFP and contract document of the proposed solution.

The Acceptance Test shall be carried out jointly by the representatives of RBI, System Integrator and the respective OEMs after the proposed solution is configured and operationalised at each site of the bank.

A comprehensive “Acceptance Test Plan (ATP)” document will be prepared in coordination with SI and OEM(s) and shall contain various aspects of the ‘Acceptance Test’ to demonstrate all the features of the proposed solution, as envisaged in this tender document and claimed by the bidder. The Acceptance Test shall be deemed to be complete only on the issuance of the ‘Acceptance Certificate’ as per **Annex XXII** by the RBI to the Bidder for the overall project by meeting the criteria mentioned in the **Annex XXIII**.

Without limiting the scope of the Acceptance Test, the test cases to be carried out in this connection should be submitted by the OEM/bidder to the Bank and subject to approval of the Bank, shall be used to assess the acceptability of the proposed solution. In general, all the features that are listed as mandatory in the RFP and selected in desirable field by the bidder should be showcased.

The UAT for hardware includes functional tests, resilience tests, benchmark comparisons, operational tests, load tests etc. The hardware should meet the technical and other specifications at the minimum, as envisaged in this document. The Bidder shall demonstrate the capabilities and perform complete testing of equipment, features and configuration of all the equipment as decided by the bank. On evaluation of the Acceptance Test results and if required in view of the performance of the proposed solution, as observed during the Acceptance Test, the Vendor shall provide necessary solution or components of the solution at his own cost thereof, to ensure the performance of the proposed solution is meeting the requirement, as envisaged in this document.

The solution provided by the Bidder must meet the technical and other specifications at the minimum, as envisaged in this document.

The Bank will accept the "Stabilisation" of the solution only on satisfactory completion of Audit, Validation & Certification by respective OEMs. The solution will not be accepted as complete if any facility/ service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP.

The Bank reserves the right to conduct third party audits, if required, for assurance.

The Go-Live (project sign-off) will be considered only after submission of OEM audit, validation & certifications by all the respective OEM/s of the proposed solution and deployment of FMS resources.

21 Contacting the Bank

No Bidder shall contact the Bank on any matter relating to its Bid, from the time of opening of Bid to the time the Contract is awarded. Any effort by any bidder to influence the Bank in its decisions on Bid evaluation, bid comparison or contract award may result in the rejection of that bidder's Bid.

22 Cost of Bidding

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

23 Bidding Document

The bidder should examine all instructions, forms, terms and conditions and technical specifications in the Bidding Document. Failure to furnish all information required by the Bidding Document or submission of a bid not fully responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of the bid without any further intimation to the bidder.

At any time prior to the deadline for submission of Bids, the Bank, for any reason, whether, at its own initiative or in response to a clarification requested by a prospective Bidder, may modify the Bidding Document, by amendment.

24 Bidding process

Instructions for Bid Submission

The entire bidding process would be conducted through the e-tendering portal of MSTC Ltd. The URL for the same is https://www.mstcecommerce.com/eprocn/ The bids should be submitted online at the website MSTC e-Procurement Portal for RBI (https://www.mstcecommerce.com/eprocn/). The bidders will have to upload the duly signed and scanned documents as part of bid. It must be ensured that all the documents are uploaded while submitting the tender online. The vendors are requested to note that they cannot make their online submission after the time stipulated above and no extension of time will normally be permitted for submission of tenders.

In case the Commercial Bid amount is indicated in any manner or form in the Bid, the Bank shall reserve the right to summarily reject the bid. The bid amount should only be indicated in the relevant annex in the Commercial Bid.

All respective bids need to be submitted through this portal only. The bidder shall exercise due care in submitting bill of material by referring to all the relevant requirements and technical specifications given in this document.

The bids will be submitted in two parts on the MSTC web portal:

a. Eligibility Criteria and Technical Bid Evaluation:

This comprises of the following to be submitted by the bidder:

Online	
S No	Documents Required for Eligibility Criteria (Stage I)
1	Bidders Profile (Annex XIV)
2	Bidder Eligibility Criteria (Necessary documents in support of this)
3	Non-Disclosure Agreement (Annex XVI) (**original to be submitted in physical to Bank**)
4	Copy of Integrity Pact document (**original to be submitted in physical to Bank**) – Annex XV
5	BG against Earnest Money Deposit (**original to be submitted in physical to Bank**) – Annex XVIII
6	Compliance Statement (Annex VIII)
7	Manufacturer Authorization Format (Annex IX)
8	Deviations (Annex VII)
	Documents Required for Technical Bid (Stage II)
1	Technical Bid Form without price (Annex IV)

2	Undertaking from Bidder on Support & Products (Annex X and Annex XII)
3	Undertaking from OEMs on Support (Annex XI)
4	Letter of Authority from OEM (Annex XXI)
5	Product Brochures containing detailed description of essential technical and performance characteristics of all offered components. This will be used in determining the compliance given to specification. Hence sufficient information is to be provided.
6	Necessary documentary evidence for Bidder's experience in implementing the similar solution in the last five years as per technical evaluation criteria. **SUMMARY DOCUMENT** to be provided listing the details of projects (project name, client, po date, items/solution, po amount, documentary proof) against all the sub-categories of implementation experience mentioned in technical evaluation criteria.
7	Compliance to Self-Declaration Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (Annex XVII)
8	Compliance to remaining Annexures of RFP

b. Commercial Evaluation response

- Commercial Bid Form - Annex VI
- Compliance Certificate of Commercial Bid (Annex XX)

Note: Bank shall upload the price bid form in Excel format on MSTC portal post pre-bid meeting to include changes, if any, on account of corrigendum.

i. The bidders are requested to note that it is mandatory to get registered with MSTC and have a valid digital certificate/signing certificate issued by any certifying authority approved by Govt. of India to participate in the online bidding. The bidders are requested to ensure that they have the same, well in advance and if any assistance is required for the purpose, bidder can contact MSTC e-Procurement team directly (Mr Tanmoy Sarkar, Deputy Manager, MSTC, +91-8349894664/022-22872011).

ii. RBI will open the bids on scheduled date mentioned in the RFP in presence of Bidders' representative. Representatives of Bidders, who choose to be present during the Bid opening on the stipulated last date and time may have to send an email from the authorised signatory of the bidder with authorisation to

represent them at the time of opening of the bids. The bids will be opened at the scheduled time, even if, the Bidder's representatives are not present at the time of opening of bids, due to what-so-ever may be the reason.

iii. The bidder should indicate unit price of each, and every component proposed by them. The prices quoted by the bidder shall be in Indian Rupees, firm and not subject to any price escalation till award of the contract.

iv. The price quoted should be all inclusive of taxes/GST. GST and/or any other tax/es need to be indicated separately, otherwise, it will be construed that the price quoted include all the applicable tax and payment will be made accordingly.

25 E-Tendering Registration and Bid submission

The Bank has entered into an agreement with MSTC Ltd. For e-tendering services, the bidder is expected to register themselves on the MSTC Ltd. E-commerce Web portal. The bidder is expected to have a Digital certificate with encryption and signing rights. The vendor registration on the MSTC Ltd. Ecommerce Web portal is present on the MSTC website. It is the bidder's responsibility to register on the MSTC Ltd. Ecommerce Web portal and obtain the necessary digital certificate. The bank shall upload the entire RFP with annexes on the MSTC Ltd. Ecommerce Web portal (http://www.mstcecommerce.com/eprochome/rbi). As per MSTC rules, applicable charges will have to be paid by the bidder.

26 General Guidelines

The Bid offers should be made strictly as per the formats specified in this RFP Document. The Bid should not contain any insertion, deletion, comments/over-writings or corrections. The content as available in the main document will only be taken for consideration. The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Documents. Failure to furnish all information required by the Bidding Documents or submission of a bid not in conformity to the Bidding Documents in every respect will be at the Bidder's risk and may result in rejection of the bid.

- No rows or columns of the bid should be left blank, **neither zero price should be quoted for any line item in the Bill of Material**.

- Bids with insufficient information which do not strictly comply with the stipulations given above, are liable for rejection.
- The Bank may, at its discretion, abandon the process of the selection of Bidder any time before notification of award.

All information (bid forms or any other information) to be submitted by the Bidders must be submitted on the MSTC Ltd. Ecommerce web portal. The Bidders may note that no information is to be furnished to the Bank through e-mail except when specifically requested by Bank, as deemed fit, may seek clarification/ information from the Bidder for evaluation purpose, however it is not obligatory on the part of the Bank to seek additional information. The Bank may choose to rely solely on the documents submitted along with the bid and complete the assessment of evaluation of the Bid.

It may be noted that all queries, clarifications, questions, relating to this RFP, technical or otherwise, should be sent by email only to the designated email id. For this purpose, communication to any other email id or through any other mode will not be entertained. The Bank reserves the right to pre-pone or post-pone the pre-bid meeting date and the revised date will be published on RBI website and also on MSTC Portal. Prospective bidders need to submit /email their queries in advance on the email given in the RFP notice.

27 Pre-Bid Meeting

- The Bank will conduct a pre-bid meeting to address the queries received form the prospective bidder's bank on the stipulated date as indicated in RFP.
- Any pre-bid queries can be sent to the designated email id as per schedule given in RFP schedule para 1.
- RBI may, at its discretion, answer such queries in the Pre-bid meeting. However, certain specific information which may comprise the secrecy and privacy for the Bank's infrastructure may not be disclosed during pre-bid meeting. Such information will be shared only with the successful bidder. If any prospective bidder needs any such confidential information, they may sign confidentiality and non-disclosure agreement to get such information.

- It may be noted that all queries, clarifications, questions, relating to this RFP, technical or otherwise, should be only to the designated email id as stated earlier. For this purpose, communication to any other email id or through any other mode will not be entertained.
- All points discussed during the pre-bid meeting, if need be, may be posted on the MSTC website along with their responses.
- No queries will be answered after Pre-bid meeting.

28 Correction of Errors

Arithmetic errors in bids will be treated as follows:

- Where there is a discrepancy between the amounts in figures and in words, the amount in words shall govern; and
- Where there is a discrepancy between the part-wise quoted amounts and the total quoted amount, the part-wise rate will govern.
- If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail.
- If there is discrepancy between unit price and total price, the unit price shall prevail for calculation of the total price.
- If there is a discrepancy in the total, the correct total shall be arrived at by Bank.

In case the Bidder does not accept the correction of the errors as stated above, the bid shall be rejected, and decision of the Bank will be firm and final.

The amount stated in the bid form, adjusted in accordance with the above procedure, shall be considered as binding, and will be considered for calculation of Final- Total Cost of Ownership (TCO).

29 Acceptance or Rejection of Bid

The Bank reserves the right not to accept any bid, or to accept or reject a particular bid at its sole discretion without assigning any reason whatsoever.

30 Duration and Condition of Engagement

Reserve Bank of India shall engage and appoint the successful Bidder to provide services as detailed in Scope of work of this document and in consideration of remuneration payable by Reserve Bank of India to the Bidder. Post implementation,

there shall be a User acceptance process to ensure all agreed deliverables are met. Post completion of warranty, the Bidder is expected to provide Support & Comprehensive AMC/ATS for two years.

The contract may be extended further as per the mutual agreement of the parties.

The Bank will reserve the right to terminate the services of the successful Bidder at any point of the Project (during the implementation phase and User acceptance) without assigning any reasons by giving a written notice of 30 days to the Vendor. In such cases the Bank may consider making payment commensurate with the last completed phase.

31 Amendments to RFP Document

Amendments to the RFP Document may be issued by the Bank for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, prior to the deadline for the submission of bids, which will be placed on the MSTC web portal with a notice on “Tender” section of RBI website.

From the date of issue, amendments to Terms and Conditions of RFP shall be deemed to form an integral part of the RFP. The amendments so placed on the MSTC web portal will be binding on all the Bidders.

32 Format and Signing of Bid

The bid should be signed by the Bidder or any person duly authorized to bind the Bidder to the contract. The signatory should give a declaration and through authenticated documentary evidence establish that he/she is empowered to sign the bid documents and bind the Bidder. All the pages of the bid should be serially numbered.

Forms with respective Power of Attorney should be submitted and digitally signed by the bidder’s representative at MSTC portal for submission of the Bid.

33 Governing Language

All correspondences and other documents pertaining to the contract shall be in English. The Contract will be signed in Bilingual, that is Hindi and English. In case of any interpretation, the version in English will prevail.

34 Applicable Law

The Contract shall be governed and interpreted in accordance with the Indian Laws and jurisdiction of the Court will be Mumbai.

35 Notices

a. Any notice given by one party to the other, pursuant to the contract shall be sent to the other party (as per the address mentioned in the contract) in writing either by hand delivery or by registered post or by courier and shall be deemed to be complete only on obtaining acknowledgement thereof; or by facsimile or by other electronic media and or mode and in which case, the notice will be complete only on confirmation of receipt by the receiver.

b. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

36 Contract Amendments

Any change made in any clause of the contract which shall modify the purview of the contract within the validity and currency of the contract shall be deemed as an Amendment. Such an amendment can and will be made and be deemed legal only when the parties to the contract provide their written consent about the amendment, subsequent to which the amendment is duly signed by the parties and shall be construed as a part of the contract. Further details of the procedure for amendment shall be as specified in the contract.

37 Confidentiality of information

Information collected by or provided to the Bidder would be treated as confidential at all times, even after expiry of the Contract and shall not be used by the Bidder for any other purpose, in contravention of the scope of work or the Contract. The work/study/deliverables carried out by the Bidder would be the sole property of the Bank excluding pre-existing IPR rights of Bidder/OEMs. Without prejudice to the confidentiality agreement which the Bidder has signed with the Bank, the Bank shall have the right to claim damages from the Bidder to the extent of the loss suffered by it, on account of the disclosure of confidential information by Bidder or its permitted assigns, at any point of time, even after expiry of the Contract and/ or take such other action against the Bidder concerned as may be appropriate and lawful. Besides, any such incident shall give an absolute right to the Bank to terminate the Contract by giving written notice to the Bidder.

The Bidder acknowledges that, during the performance of this Contract, Bank may disclose certain confidential information to Bidder for the performance of this Contract. For purpose of this Contract, the term “Confidential Information” means any and all oral or written information that is not generally or publicly known and that which the Bidder has obtained pursuant to this Contract and the term “Confidential Information” shall include, but shall not be limited to, papers, documents, writings, classified information, inventions, discoveries, know how, ideas, computer programs, source codes, object codes, designs, algorithms, processes and structures, product information, research and development information and other information relating thereto, financial data and information and processes of a business, commercial, technical, scientific, operational, administrative, financial, marketing or intellectual property nature or otherwise and anyother information that Bank may disclose to Bidder, or that Bidder may come to know by virtue of this Contract. Confidential Information also includes information obtained and provided by Bidder in confidence from third parties, including, but not limited to, its sub-contractors,consultants, or clients and any other information of a private, confidential or secret nature concerning RBI, whether or not relating to the affairs of RBI.

Bidder acknowledges that any information obtained from the Bank and not publicly known shall be treated as confidential and shall not be disclosed to any third party without the other Party's prior consent. Such confidentiality obligation is not applicable if the disclosure of information is required by law or regulation. However, any Party compelled to disclose by law or regulation or by any court of competent jurisdiction, upon being so compelled to disclose, shall notify the other Party in writing forthwith, unless prohibited by law. Such confidentiality obligation is also not applicable if such disclosure is made to their directors, officers, auditors, lawyers, consultants who needs to know such information during the ordinary course of business, however, intimation with adequate notice must be given.

The Bidder agrees and undertakes to hold the Confidential Information in strict confidence and take all reasonable steps necessary (including but not limited to those required hereunder) to preserve such confidentiality. The Bidder covenants and agrees with Bank that it will not, during the term of the Contract and thereafter, perpetually, directly or indirectly use, communicate, disclose or disseminate to anyone any

Confidential Information and any other information concerning the businesses or affairs of Bidder that the Bidder may have acquired in the course of or as incidental to Bidder engagement or dealings with Bank other than with prior written consent of Bank.

The Bidder shall not, without the Bank's prior written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the Bidder in the performance of the Contract, to whom also it shall be on 'need to know' basis and to the extent permitted under this Contract. Disclosure to any such employed person shall be made in confidence and where such employees are bound by similar confidentiality obligations as set out in this Contract.

Any document, other than the Contract itself, shall remain the property of the Bank and all copies thereof shall be returned to the Bank on termination of the Contract.

The Bidder shall ensure that all its employees, agents and sub-contractors involved in the project, execute individual non-disclosure agreements, with respect to this Project. The Bidder may submit a declaration that it has obtained the NDA from its employees. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

- information already available in the public domain;
- information which has been developed independently by the Bidder;
- information which has been received from a third party who had the right to disclose the aforesaid information;
- information which has been disclosed to the public pursuant to a court order.

38 Force Majeure

Neither Party shall be liable for any act, omission, failure or delay in fulfilling its obligations under this Contract arising out of or, caused directly or indirectly by any unforeseen event, or a cause reasonably beyond its control; including but not limited to vis major (Force Majeure event) such as natural phenomenon, including but not limited to floods, droughts, earthquakes, pandemics, or any other event reasonably beyond the control of any of the Parties.

The Party unable to fulfil its obligations due to a Force Majeure event shall within reasonable time notify the other Party in writing of the Force Majeure event, the extent to which the Force Majeure event prevents fulfilment of its obligations with reasons thereof; and the estimated duration of the subsistence and effects of the Force Majeure Event; and use best endeavours to expedite fulfilment of its obligations and in the meantime, mitigate the effect(s) of such Force Majeure event.

39 Integrity Pact

As a part of the implementation of Integrity Pact programme in the Bank all bids will be covered under the Integrity Pact and the vendors are required to sign the Integrity Pact document and submit the same to the Bank along with the bids.

i. All bidders need to sign the Integrity Pact before the bids are opened by the Bank. Bids without the signed Integrity pact are liable to be rejected.
ii. Only those vendors who have signed the Integrity Pact document and submitted the bid can send their queries, if any, to
iii. Bidders are requested to sign the Integrity pact as per the relevant Annex.

The Integrity Pact envisages, if required, the appointment of an Independent External Monitor (IEM) who would independently review the extent to which the two parties to the contract (the bidder and the Bank) have complied with their obligations under the Integrity Pact. As approved by the Central Vigilance Commission, Shri Nageshwar Rao Koripalli, IRS (Retd.) (Email: nageshwarrao@gmail.com) and Shri Pramod Shripad Phalnikar, IPS (Retd.) (Email: pramodphalnikar@gmail.com) have been appointed as Independent External Monitors (IEMs) in RBI, either of them may act as IEM for this RFP process. The bidder may contact them at their respective email IDs.

40 Subcontracting

The Bidder shall not subcontract or permit anyone other than its personnel and the parties enlisted in the response to perform any of the work, service or other performance required of the Bidder under the contract without the prior written consent of the Bank.

41 Indemnity to the Bank

The successful Bidder shall, at its own cost and expenses, defend and indemnify the Bank against all third-party claims including those of the infringement of Intellectual

Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India or outside India.

If the Bank is required to pay compensation to a third party resulting from such infringement, the Successful Bidder shall be fully responsible therefore, including all expenses and court and legal fees. The Bank will give notice to the successful Bidder of any such claim and shall provide reasonable assistance to the Successful Bidder in disposing of the claim. Vendor shall have sole responsibility over the defence of any such claim.

42 Cancellation of Contract and Compensation

The general rule is that neither party to a contract may avoid performance of its duties to the other unless the other party first materially breaches the contract. For example, a System Integrator may not refuse to perform its work under a contract unless the Reserve Bank does something that would constitute a material breach, such as failing to make payments in accordance with the agreed upon payment terms. Similarly, in the absence of a material breach by a System Integrator, the Reserve Bank cannot simply terminate the contract.

The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank on the following circumstances:

a. The selected Bidder commits a breach of any of the terms and conditions of the bid/contract.
b. The Bidder goes into liquidation voluntarily or otherwise.
c. The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.
d. The parties fail to settle the matter accordance with Dispute Resolution Mechanism mentioned in this contract.
e. If the contractor fails to perform any other obligation under the contract within the period specified in the contract or any extension thereof granted

After the award of the contract, if the selected Bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month’s notice for the same. In this event, the bidder is bound to make good the additional expenditure, which the Bank

may have to incur to carry out bidding process for the execution of the balance of the contract.

The Bank reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected Bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order. Work, Study Reports, documents, etc. prepared under this contract will become the property of the Reserve Bank of India.

In cases, where RBI is terminating the contract, RBI would pay the bidder for the services, hardware, software and AMC /ATS rendered till the last day of termination after adjustment of dues as at above.

The Bidder reserves the right to cancel the contract with a written notice of 30 calendar days to the Bank. The Bank will not make any payments if any milestones have not been achieved and has the right to recover any advance payments made. The Bank shall pay for goods delivered and services rendered till the date of termination after recovery of any applicable dues payable by the selected Bidder.

43 Dispute Resolution Mechanism

The Vendor and RBI shall always endeavour to amicably settle all disputes arising out of or in connection with the Contract. In the event of any dispute, controversy or claim arising out of or relating to this Contract, or any alleged breach hereof, that may arise in between the Parties in connection with this Contract, the Parties shall first attempt to settle the same through negotiations between representatives authorized for this. Parties shall use best endeavours to conclude the process of negotiations within a period of 30 days from the date on which any Party gives the other Party a notice to negotiate in good faith.

In the event negotiations fail, the dispute shall then be referred to and finally resolved by arbitration and the dispute may be submitted by either Party. The law governing this arbitration clause shall be Arbitration and Conciliation Act, 1996. The seat of arbitration shall be Mumbai, Maharashtra, India. The arbitral tribunal shall comprise of three arbitrators (each Party to choose one, and the third to be appointed by mutual consent). The language of arbitral proceedings shall be English.

While identifying for appointment of the Arbitrator, the parties and the arbitrators, as the case may be, shall take into consideration the type of services envisaged under this Contract and the nature of dispute that is sought to be resolved. The “Arbitration Notice” issued by either Party should accurately set out the disputes between the Parties, the intention of the aggrieved Party to refer such disputes to arbitration as provided herein, the name of the person it seeks to appoint as an arbitrator with a request to the other Party to appoint its arbitrator within 30 days from receipt of the notice. All notices by one Party to the other in connection with the arbitration shall be in writing.

Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides. The Vendor shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service/s in accordance with the provisions of the Contract/Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings. The Bank will continue to pay the Vendor for such services rendered during pendency of disputes. However, the Bank reserves its right to withhold / temporarily terminate the services of the Vendor if it deems fit, depending on the nature of the dispute and the circumstances surrounding it.

44 Taxes and Duties

The Bidder shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed within and outside India.

The Bidder is expected to submit the Commercial bid inclusive of all taxes including applicable GST for each line item as mentioned in the format in the relevant Annex.

The calculation of the applicable taxes and other levies should be shown separately.

In case of any new taxes or duties and revision of existing taxes and duties, if any, introduced by Government of India or State government after the award of contract to the System Integrator, shall be paid separately by RBI on actuals (on submission of documentary proof). Benefit realised, by the System Integrator, if any, due to reduction in rate of taxes/duties/levies/charges shall be passed on to Bank.

45 Notification of Awards

The acceptance of a bid, subject to contract, will be communicated in writing at the address supplied by the Bidder in the bid response. Any change of address of the Bidder, should therefore be promptly notified to:

The Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

46 Authorized Signatory for signing the contract

The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the Bank, with regard to the obligations under the contract. The authorized signatory should give a declaration and through authenticated documentary evidence establish that he/she is empowered to sign the bid documents and bind the bidder. The Bidder shall furnish proof of signature identification for the above purposes as required by the Bank.

47 Signing of Contract

The Successful Bidder shall be required to enter into a contract with Reserve Bank of India, within **45** working days of the issue of the Purchase Order or within such extended period mutually agreed by both parties. All cost (legal charges like cost of stamp duty etc) associated with the preparation/signing the agreement shall be borne by the successful bidder.

48 Vicarious Liability

The Bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the Bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc., by the Bidder, for any assignment under the contract. All remuneration, claims, wages dues etc., of such employees, agents, contractors, subcontractors etc., of the Bidder shall be

paid by the Bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the Bidder's employees, agents, contractors, subcontractors etc. The Bidder shall agree to hold the Bank, its successors, assignees and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, that may arise from whatsoever nature (on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Bank) through the action of Bidder's employees, agents, contractors, subcontractors etc. in performance or non-performance under this Agreement.

49 Assignment or transfer of contract

Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the Bidder, and any such attempted sale, lease, assignment or otherwise transfer shall be void and of no effect without the advance written consent of the Bank.

50 Survival of Clauses

The provisions relating to indemnity, confidentiality, Deliverables, limitation of liability, governing law and jurisdiction and any clause that by its reasonable implication is intended to survive, shall survive termination of the awarded Contract.

51 Non-Solicitation

Neither the Bidder nor RBI, during the term of the contract and for a period of two years thereafter shall without the express written consent of the other party, directly or indirectly:

i Recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services under the contract; or

ii Induce any person who is / have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

iii Provided that this clause shall not restrict the right of the Party from recruiting generally in the media and shall not prohibit the Party from hiring any employee of other Party who answers any advertisement

without having been initially personally solicited or recruited by the hiring Party.

52 No Employer-Employee Relationship

i. The Bidder or any of its holding/subsidiary/joint-venture/ affiliate / group / client companies or any of their employees / officers / staff / personnel / representatives / agents shall not, under any circumstances, have /deemed to have any employer-employee relationship with the Bank or any of its employees /officers / staff / representatives / personnel / agents.

ii. A self-declaration is required from the bidder as part of the technical bid.

53 Insurance Coverage

The bidder is required to take Transit Insurance and Erection All Risk (EAR) policy to cover cost of the entire hardware and/or software equipment at respective RBI location for up to 45 days from the date of delivery. Please note that insurance premium amount needs to be borne by the bidder only.

The bidder shall maintain at its expense all statutory mandated insurance such as workers' compensation and employer's liability. The bidder shall submit a declaration signed by their authorised signatory in this regard.

54 Fixed and Non-negotiable pricing

Prices quoted must be firm and final and shall not be subject to any re-openers or upward modifications, on any account whatsoever including exchange rate fluctuations during the contract period. Prices must be indicated in Indian Rupees (INR) only.

55 Compliance with Local Conditions

It will be imperative on each Bidder to fully acquaint himself with the local conditions and factors, which would have any effect on the performance of the contract and / or the cost. It is responsibility of each Bidder to fully inform themselves of all legal conditions and factors which may have any effect on the execution of the contract as described in the Bid Documents. Bank shall not entertain any request for clarification from the Bidder regarding such local conditions. It is the responsibility of the Bidder that such factors have properly been investigated and considered while submitting the bid proposals and that no claim whatsoever including those for financial adjustment to the contract awarded under the Bid Documents will be entertained by Bank and that neither any change in the time schedule of the contract nor any financial adjustments

arising thereof shall be permitted by Bank on account of failure of the bidder to appraise themselves of local laws / conditions.

56 Information Security

The Bidder and its personnel shall not carry any written material, layout, diagrams, CD/DVD, hard disk, storage tapes or any other media out of RBI's premise without written permission from the RBI. The Bidder personnel shall follow the Bank's information security policy and instructions in this behalf.

Bidder shall provide certificate/assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

The Bidder shall ensure that the equipment / application / software and future upgrades being supplied shall be free from malicious code (Viruses, Trojan, Spyware etc.) and shall be liable for any loss (information, data, equipment, theft of Intellectual Property Rights, network breach, sabotage etc.) incurred to the bank arising due to activation of any such embedded malware / malicious code. The bidder shall ensure that subsequent patch, hot fixes and upgrades are also free from malicious code.

57 Ownership and Retention of Documents

The Purchaser shall own the documents, prepared by or for the Bidder arising out of or in connection with this Contract.

Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by RBI, the Bidder shall deliver to the Purchaser all documents provided by or originating from RBI and all documents produced by or from or for the Bidder in the course of performing the Services, unless otherwise directed in writing by RBI at no additional cost. The Bidder shall not, without the prior written consent of RBI store, copy, distribute or retain any such Documents.

58 Manuals

The Bidder must along with the equipment, supply all relevant manuals for the systems delivered / installed. The manuals shall be in English. Unless and otherwise agreed, the equipment(s) shall not be considered completely delivered for the purpose of taking over, until such manuals as may be necessary are provided to Purchaser. System manuals should include the specifications of the various equipment supplied.

59 Sexual Harassment Clause

The Vendor shall be solely responsible for full compliance with the provision of the Sexual harassment of women at workplace (Preventions, Prohibition and Redressal) Act, 2013 and further amendments, if any. In case of any complaint of sexual harassment against its employee within the premises of the Bank, the complaint shall be filed before the Internal Complaints Committee constituted by the Vendor and the Vendor shall ensure appropriate action under the said Act in respect to the complaint. Vendor shall be responsible for any monetary compensation that may need to be paid in case the incident involves the employees of the Vendor. The Vendor shall provide a complete list of its employees, updated from time to time, who will be providing services to the Bank.

60 Governing Law and Jurisdiction

The validity, interpretation, construction and performance of this Contract shall be governed by Indian Laws and Courts in Mumbai shall have exclusive jurisdiction.

61 Limitation of Liability

The Vendor's aggregate liability in connection with obligations undertaken as a part of this Contract 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 excluding taxes.

62 Restriction on Procurement due to National Security

Compliance with the Rule 144(xi) of GFR 2017 inserted vide Office Memorandum (OM) OM No. F7/10/2021-PPD dated February 23, 2023 issued by 'Public Procurement Division, Department of Expenditure, Ministry of Finance, Government of India, the Public Procurement Orders issued in furtherance thereto, and their subsequent revisions shall be mandatory. In this regard, Bidder shall submit a copy of Undertaking / Declaration / Certificate on their letter head duly sealed and signed by the authorized signatory in the format at as per Annex II.

If the Undertaking / Declaration I Certificate submitted by the bidder is found to be false, his/her/its tender/ work order will be immediately terminated, and legal action in accordance with law including forfeiting of Earnest Money Deposit/ Performance Bank Guarantee/ Security Deposit may be initiated and the Bank may also debar the bidder from participating in the tenders invited by the Bank in future.

List of RBI locations

S No	Location
1	Site – 1 Far DR Data Centre- Nagpur
2	Site – 2 Primary Data Centre – Navi Mumbai
3	Site – 3 Near DR Data Centre- Navi Mumbai
4	Site – 4 Next Generation Greenfield Data Centre – Bhubaneswar
5.	Any other location proposed by Bank

Annex II - Proforma for Undertaking/ Declaration/ Certificate by the bidder/OEM regarding country sharing land border with India

To be submitted by bidder on their letter head duly sealed and signed by the authorized signatory

The Chief General Manager-in-Charge
Department of Information Technology,
Central Office, Reserve Bank of India,
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai – 400 001.

Dear Sir,

Ref: RFP No. _____dated _____
Bidder Name: _____

I / We _____ (Name and address, including Country of location of bidder/OEM) have read and understood and are in compliance with the contents of the Office Memorandum OM No. F7/10/2021-PPD dated February 23, 2023, and its subsequent orders/revision issued by Public Procurement Division, Department of Expenditure, Ministry of Finance, Government of India regarding the restrictions on procurement from a bidder of a country which shares a land border with India.

2. I/We further certify that _____ (Name of bidder/OEM) fulfils all requirements in this regard and is eligible to be considered under the provision of the above referred Office Memorandum and its subsequent orders/ revision. I/We also undertake that even in case of contracts where we are permitted by the Bank/RBI to sub- contract. I/we _____ (Name of bidder/OEM) will not sub-contract any work to a contractor from country(ies) sharing land border with India, unless such contractor fulfils all the requirements contained in the above referred office memorandum / order.

3. I/We know and understand that, if this Undertaking / Declaration / Certificate submitted by us is found to be false, the Bank shall be free to reject/ terminate our tender/ Work Order and that the Bank shall also be free to initiate any legal action in accordance with law including forfeiting of Earnest Money Deposit / Performance Bank

Guarantee / Security Deposit and / or debarring us from participating in tenders invited by the Bank in future.

Signature and name of the authorized signatory of the Bidder with Rubber Stamp

Date:

Place:

The list of features required for each solution is as below:

A. Internal Firewall - MZ / Internal Firewall

Sr. No.	Mandatory Requirements	Compliance (Y/N)
1	The device should be capable to manage load and perform functions of Firewall and IPS.	
2	**Hardware, Performance and Capacity:** The firewall must have the following capacity for the below mentioned parameters: i. HTTP Throughput with a packet size of 1024 byte → 35 Gbps ii. Threat Prevention Throughput with SSL Inspection of 90% of the total throughput/traffic → 15 Gbps iii. Concurrent TCP/HTTP Connection Capacity: 7.5 Million concurrent sessions iv. TCP/HTTP Connections Per Second: 2.5 lakhs new sessions per second v. The following features of the Next Generation Firewall must be enabled while the benchmark testing is carried out: a) SSL Inspection- must be supported for 90% of the total throughput/traffic. b) IDS & IPS c) Anti-Spyware d) Anti-Botnet e) Anti-Malware f) Logging and Reporting g) Application Identification h) Firewall The values of the above-mentioned parameters for the proposed firewall model need to be validated by the OEM on their letter Head and signed by the Authorised signatory. The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device Performance' dated March, 2023. The test report which is attested by the authorised signatory of the OEM shall be submitted as a supporting document for compliance to this requirement. vi. The firewall must have a minimum of 192 GB of memory. vii. The storage provided in the Firewall must be	

	Flash/SSD type storage. viii. The Firewall must have Minimum of 4 x 1G copper RJ45 ports, 4 x 40G SFP+, 4 x 10G and 4 x 100G SFP+ ports with necessary transceivers from day one. ix. High Availability, Sync & Management port shall be provided separately. x. The NGFW hardware must have redundant and hot swappable hardware components like power supply, fan, etc.	
3	The NGFW must provide the following features from day one: a) SSL Inspection- must be supported for 90% of the total throughput/traffic. The NGFW must provide SSL inspection feature for specific or selective traffic based on source/destination IP and Application b) IDS & IPS c) Anti-Spyware d) Anti-Botnet e) Anti-Malware f) Logging and Reporting g) Application Identification h) Packet Capture utility with Support for IPV4 and IPV6 i) QoS Marking j) Policy based Forwarding The licensing structure for the features must be clearly spelt out in the technical Bid document and Bill of Materials. Any of the features that are provided in addition to the above-mentioned features must also be clearly indicated along with the license structure in the technical bid document.	
4	**High Availability Configuration:** The NGFW must be deployed in High Availability (HA) pairs in Active - Passive configuration and must support high availability for both IPV4 & IPV6 traffic. The failover between the HA pairs must be seamless and automatic without requirement for manual intervention.	
5	**Central Management:** i. The NGFW solution must provide for a common central management console for all firewalls. ii. The Central Management Appliance must support 3 TB storage from day one. iii. If the appliance is virtual, the compute and storage for the virtual appliance will be provided by the Bank. iv. The OEM must provide 2 Central Management Appliances at two different sites capable to manage all its NGFW devices. v. Operations, Reporting, policy/rule creation & deployment, alerts management, security configuration, etc. must be managed from the same management	

	server. vi. Management server should be able to provide an exportable Graphical report for all the audit changes done by the administrators between previous and currently installed policy version/s including changes on Rules, Policies, objects, etc. vii. The Central Management console must have the following features from day one: a) Integrate with existing Ticketing System (Microfocus Service Management Automation X) b) Risk Analysis of Firewall Rules based on RBI's own current Risk Matrix which will learn and develop on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc. c) Firewall rules optimisation: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets d) Integrate with existing Vulnerability Assessment tool to co-relate Firewall Risky Rules & Vulnerability data to assess the attack surface.	
6	**Migration & Integration** The solution must provide seamless approach to migrate existing policies, signature database, etc. without any disruption. The solution must integrate with the existing security and monitoring solutions in the Bank viz. PIM, SIEM, SOAR and NTA, and Network Node Monitoring tool.	
7	The NGFW solution architecture should have Control Plane separated from the Data Plane whereby Control Plane should handle Management functions and Data Plane should handle security processing and network processing functions. Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure that Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture	

	etc to identify the root cause and accordingly take necessary action to remediate it.	
	Desirable Features	**Marks**
8	The NGFW should acquire User Identities from LDAP.	**10**
9	The proposed solution must provide detailed information on each protection, including Vulnerability and threat descriptions, including CVE details & Threat severity.	**10**
10	The NGFW solution should provide : a) QoS Marking (16 marks) i. by source address (2) ii. by destination address (2) iii. by application (such as Webex, Social Media) (4) iv. by static or dynamic application groups (such as Instant Messaging or P2P groups) (2) v. by port (2) vi. by services (4) b) Policy based Forwarding (16 marks) i. Based on Zone (2) ii. Source or Destination Address (2) iii. Source or destination port (2) iv. Application (not port based) (4) v. AD/LDAP user or User Group (2) vi. Services (4)	**32**
11	**Load Balancing & Auto Failover of Links/paths:** The NGFW solution must provide for load balancing and Auto Failover of minimum four (4) links/paths. The load balancing and automatic failover must be seamless and automatic without manual Intervention.	**12**
12	Central Management Console: The Firewall Central Management solution should have following features: The management solution should provide customisable Management Dashboard - to provide quick insight about i) Applications , ii) Users , iii) Files, iv) Top Rule Usage, v) Content, vi) Threat classification/category	**18 (3*6)**
13	Application Awareness: 1. The solution should have 6000+ applications in their application aware database. (3) 2. The solution should have 5000-6000 applications in their application aware database. (2) 3. The solution should have 4000-5000 applications in their application aware database. (1)	**9 (3*3)**
14	IPS Signatures: 1. The solution should have 18,001+ IPS Signatures. (3) 2. The solution should have 15,001-18000 IPS Signatures. (2)	**9 (3*3)**

	3. The solution should have 10,000-15000 IPS Signatures. (1)	
Total		**100**

B. External Firewall (different OEM) – Perimeter, DMZ, Management and Backbone Firewalls:

S.N.	Mandatory Requirements	Compliance (Y/N)
1	The device should be capable to manage load and perform functions of Firewall, IPS and Proxy.	
2	The device should integrate with SSLO.	
3	**Hardware, Performance and Capacity:** The firewall must have the following capacity for the below mentioned parameters: i. HTTP Throughput with a packet size of 1024 byte → 35 Gbps ii. Threat Prevention Throughput with SSL Inspection of 90% of the total throughput/traffic → 15 Gbps iii. Concurrent TCP/HTTP Connection Capacity: 7.5 Million concurrent sessions iv. TCP/HTTP Connections Per Second: 2.5 lakhs new sessions per second v. The following features of the Next Generation Firewall must be enabled while the benchmark testing is carried out: a) SSL Inspection- must be supported for 90% of the total throughput/traffic. b) IDS & IPS c) Anti-Spyware d) Anti-Botnet e) Anti-Malware f) Logging and Reporting g) Application Identification h) Firewall i) URL Filtering j) Proxy functionality & traffic redirection using a PAC file (In proxy mode the device should support a minimum of 1000 concurrent session per device) The values of the above-mentioned parameters for the proposed firewall model need to be validated by the OEM on their letter Head and signed by the Authorised signatory. The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for	

	Network Security Device Performance' dated March 2023. The test report which is attested by the authorised signatory of the OEM shall be submitted as a supporting document for compliance to this requirement. vi. The firewall must have a minimum of 192 GB of memory. vii. The storage provided in the Firewall must be Flash/SSD type storage. viii. The Firewall must have Minimum of - 4 x 1G copper RJ45 ports, 12 x 10G, 4 x 40G/100G SFP+ with necessary transceivers from day one. ix. High Availability, Sync & Management port shall be provided separately. x. The NGFW hardware must have redundant and hot swappable hardware components like power supply, fan, etc. xi. The NGFW must support creating 5 virtual instances.	
4	The NGFW must provide the following features from day one: a) SSL Inspection- must be supported for 90% of the total throughput/traffic. The NGFW must provide SSL inspection feature for specific or selective traffic based on source/destination IP and Application b) IDS & IPS c) Anti-Spyware d) Anti-Botnet e) Anti-Malware f) Logging and Reporting g) Application Identification h) Packet Capture utility with Support for IPV4 and IPV6 i) QoS Marking j) Policy based Forwarding k) URL Filtering l) Proxy functionality & traffic redirection using a PAC file as a native functionality of firewall. The licensing structure for the features must be clearly spelt out in the technical Bid document and Bill of Materials. Any of the features that are provided in addition to the above-mentioned features must also be clearly indicated along with the license structure in the technical bid document.	
5	**High Availability Configuration:** The NGFW must be deployed in High Availability (HA) pairs in Active - Passive configuration and must support high availability for both IPV4 & IPV6 traffic. The failover between the HA pairs must be seamless and automatic without requirement for manual intervention.	

6	**Load Balancing & Auto Failover of ISP Links:** The NGFW solution must provide for load balancing and Auto Failover of minimum four (4) ISP links. The load balancing and automatic failover must be seamless and automatic without manual Intervention.		
7	**Central Management:** i. The NGFW solution must provide for a common central management console for all firewalls. ii. The Central Management Appliance must support 3 TB storage from day one. iii. If the appliance is virtual, the compute and storage for the virtual appliance will be provided by the Bank. iv. The OEM must provide 2 Central Management Appliances at two different sites capable to manage all its NGFW devices. v. Operations, Reporting, policy/rule creation & deployment, alerts management, security configuration, etc. must be managed from the same management server. vi. Management server should be able to provide an exportable Graphical report for all the audit changes done by the administrators between previous and currently installed policy version/s including changes on Rules, Policies, objects, etc. vii. The Central Management console must have the following features from day one: a) Integrate with existing Ticketing System (Microfocus Service Management Automation X) b) Risk Analysis of Firewall Rules based on RBI's own current Risk Matrix which will learn and develop on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc. c) Firewall rules optimisation: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets d) Integrate with existing Vulnerability Assessment tool to co-relate Firewall Risky Rules & Vulnerability data to assess the attack surface.		

8	**Migration & Integration** The solution must provide seamless approach to migrate existing policies, signature database, etc. without any disruption. The solution must integrate with the existing security and monitoring solutions in the Bank viz. PIM, SIEM, SOAR and NTA, and Network Node Monitoring tool.	
9	The NGFW solution architecture should have Control Plane separated from the Data Plane whereby Control Plane should handle Management functions and Data Plane should handle security processing and network processing functions. Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure that Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it.	
	Desirable Features	**Marks**
10	i. The NGFW should acquire User Identities from LDAP. ii. Dynamic/Retrospective Analysis in network to observe files and assess the current status of the threat as they execute in a purpose-built, evasion-resistant virtual environment, enabling detection of previously unknown malware using behavioural characteristics.	**4+4 =8**
11	i. The NGFW should block the traffic based on geo location (country wise, etc.). ii. The geo location-based configuration should be supported granularly for per policy and per application wise as per the business requirement.	**4+4 =8**
12	The proposed solution must provide detailed information on each protection, including Vulnerability and threat descriptions, including CVE details & Threat severity.	**3**

13	The NGFW solution should provide: a) QoS Marking (16 marks) i. by source address (2) ii. by destination address (2) iii. by application (such as Webex, Social Media) (4) iv. by static or dynamic application groups (such as Instant Messaging or P2P groups) (2) v. by port (2) vi. by services (4) b) Policy based Forwarding (16 marks) i. Based on Zone (2) ii. Source or Destination Address (2) iii. Source or destination port (2) iv. Application (not port based) (4) v. AD/LDAP user or User Group (2) vi. Services (4)	**32**
14	The internet link load balancing should also support the following features: i. The NGFW should support balanced round robin - equal load on the links and weighted round robin - differential loads on links based on weights. ii. Network Path Monitoring: The NGFW should have the feature of Network Path Monitoring. i.e track the health & availability of entire path including Internet Router LAN Port, WAN Port, ISP Next Hop Router IP, ISP Cloud Service & Internet Service. In case of any component failure, NGFW should detect it immediately & provide complete information about which component has failed along the path such as Internet Router WAN port OR ISP service etc. iii. The NGFW should support Symmetric Return to cause return packets to egress out the same interface on which the associated ingress packets arrived.	**3+5+3 =11**
15	Central Management Console: The Firewall Central Management solution should have following features: The management solution should provide customisable Management Dashboard - to provide quick insight about i) Applications, ii) Users , iii) Files, iv) Top Rule Usage, v) Content, vi) Threat classification/category	**12 (2*6)**
16	The solution should have capability to identify unknown C2 requests in real time to protect against C2 communications which don't have signatures in place. This functionality should be in real time & inline to be able to provide patient zero protection.	**5**
17	The solution should have capability to classify unknown URL categories in real time & inline, if there is URL which is in the unknown category the URL filtering should have capability to classify it based on the web page content inline & in real time.	**5**

18	The solution should have capability to find malicious content in real time. For example, if a allowed web page is compromised, the solution should detect malicious content in real time & should block access. This should be applicable to the content being downloaded & also the web page itself.	**5**
19	The solution has capability to analyse executable files for unknown malware in real time inline. The solution should use the AI/ML models to offer patient zero protection against unknown malware.	**5**
20	Application Awareness: 1. The solution should have 6000+ applications in their application aware database. (3) 2. The solution should have 5000-6000 applications in their application aware database. (2) 3. The solution should have 4000-5000 applications in their application aware database. (1)	**3 (1*3)**
21	IPS Signatures: 1. The solution should have 18,001+ IPS Signatures. (3) 2. The solution should have 15,001-18000 IPS Signatures. (2) 3. The solution should have 10,000-15000 IPS Signatures. (1)	**3 (1*3)**
Total		**100**

C. Malware Sandboxing for Firewalls

Sr. No.	Mandatory Features	Compliance (Y/N)
1	Sandbox to provide on premise threat analysis environment, detonation, and automated orchestration of prevention for highly evasive zero-day exploits and malware.	
2	The proposed Sandbox need to handle all the NGFWs of the respective OEMs.	
3	Features of Sandbox: a) Physical or Virtual Appliance b) Proposed sandbox solution must provide on- premises Sandbox supporting minimum 6xWin-10 OS concurrent VM Sandbox licenses c) Mitre - ATT&CK based reporting to provide malware tactics and techniques d) Payload analysis- o Classification of custom-malware, unknown, targeted and advanced threats. Creates signatures for use by IPS. o Sniffer mode, API or integrated. e) Advanced file analysis with URL crawling to prevent multi-stage, multi-hop attacks. f) Proposed OEM Sandbox must be able to scan minimum	

	10000 files using pre-filters and minimum 200 Zero day files over VM sandboxing environment per day. g) Type of Files to be handled – o Productivity (Word, Excel, PDF) o Archives (.rar, .zip, .tar.gz, .cab) o Executables (.exe, .dll, .msi) h) Protocols o HTTP, FTP, POP3, IMAP, SMTP, SMB, IM o SSL equivalent versions **The Bidder must indicate scalability metrices for various scalable bands along with cost in the commercial bid.**	

D. Web Application Firewall (WAF)

Sr. No.	Mandatory Features	Compliance (Y/N)
A	**Solution Deployment and Compatibility**	
1	The appliance should be purpose-built hardware as a single device or cluster of appliances or chassis with all components of the solution from same OEM. The Hardware should be fully multi-tenant which can support Virtual machine or container architecture.	
2	Solution should be able to work in High Availability (HA) mode (in both layer 3 and layer 2 deployments) and should be deployable in an Active-Active or Active-Standby (as per Bank's discretion) and capable of handling application traffic simultaneously. The failover should be transparent to other networking devices without any drop or break of user SSL sessions. Solution should not have any single point of failure like power supplies and fans etc.	
3	Solution should support deployment as inline mode layer 2 bridge, inline mode layer 3 proxy, out of band mode etc types.	
B	**Hardware requirements**	
1	Solution should have minimum 16 ports of 25G/10G Populated with 10G SR SFP+ and should support conversion of same above ports to 16*25G in future if required.	
2	The solution should be supplied with console port and dedicated out-of-band management port	
3	Each virtual instance should be able to work independently in high availability on the same hardware pair. This should not compromise performance and efficacy of solution.	
4	The proposed appliance should provide minimum 1.5 Gbps of real world WAF throughput (with CPU utilisation of maximum 40 percent) from day 1 and should be scalable to 3 Gbps in future (with license upgrade) on the same hardware or additional blades	

	in case of a chassis-based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per instance in blocking mode SSL inspection.	
5	The solution should have ability to upgrade / Downgrade devices software.	
6	The solution must support minimum SSL TPS/CPS: -80 K ECDSA P-256-bit keys -110 K RSA 2048-bit keys scalable to minimum SSL TPS/CPS -100 K ECDSA P-256-bit keys -190 K of RSA 2048-bit Keys	
7	The solution must have TLSv1.1 and TLSv1.2 and TLSv1.3 on both client and server side.	
C	**Capabilities to cater Bank's requirements**	
1	HA should support automatic and manual synchronization of configuration from primary HW/instance to secondary HW/instance.	
2	Solution should support manual/offline as well as automatic online updates of the signatures and updation should be not cause any downtime. Signature updation should be independent of the underlying firmware OS.	
D	**Integration Capabilities**	
1	Solution should support integration with banks SIEM, SOAR, web application vulnerability solution deployed by Bank to virtually patch web application vulnerabilities and management solutions.	
2	Solution must support external authentication including LDAP./ LDAPS, TACACS+, RADIUS etc.	
3	Solution must have seamless integration capabilities with SSLO solution proposed as part of this RFP.	
4	Solution should support ICAP, API or other supporting integration with different security devices for file scanning, sandboxing request etc.	
E	**Technical capabilities**	
1	Solution should identify and mitigate OWASP top 10, API, Automated threats, CVE signature top 25 and other qualified web application, API based vulnerabilities attacks and pattern and signatures. It should also provide OWASP compliance dashboard (application wise compliance status).	
2	Solution should support API security including support for uploading swagger file. Solution should able to discover new API paths/Shadow paths / stale API paths / Authenticated paths / Un authenticated paths.	
3	Solution should have Correlated Attack Validation capacity or Correlation 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.	

4	When deployed as full proxy mode, the Web application firewall should be able to digitally sign cookies, encrypt cookies and to rewrite URL's.	
5	Solution should provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks. Solution should provide encryption for user input fields to protect from browser-based malwares stealing users credentials.	
6	Solution should have capability to protect applications from attacks and redirect Brute Force attack traffic to Honey Pot page.	
7	Solution should have ability to automatically detect software/Server technology used on backend side to define signature sets required for defined Proposed Solution policy.	
8	Solution should identify WebSockets connections and provide security for Web sockets including security for exploit against Server abuse, login enforcement, XSS and SQL injection. The Solution should parse and monitor JSON data over web socket protocol.	
9	Solution should support WebSocket per URL message handling capabilities with no limit for frame size. Solution should also support to select message payload format e.g. plain text, JSON Binary etc.	
10	Solution should support user tracking using both form-based and certificate-based user authentication.	
11	Solution should be able to decrypt, analyse traffic and again re-encrypt before forwarding	
12	Solution should protect web applications that include Web services (XML) content (similar to the web application protection).	
13	Solution should have ability to configure way to analyse request payload based on custom rules for each URL entry configured in the security policy.	
14	Solution should support security policy to be applied per application, rather than one single policy for an entire system. Solution should not have any kind of restriction in terms of numbers of applications that can be protected, concurrent connection, bandwidth per tunnel/device.	
15	The solution should be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	
F	**Dashboard, User management and Reporting features**	
1	Solution should be capable of hosting multiple backend on single virtual IP and should be capable of identifying SNI values to make a forwarding decision/ apply a specific WAF/BoT/L7 policy (based on SNI value).	
2	Solution should have a dedicated centralized management to manage multiple WAF appliances / instances for day to day operations.	
3	Solution should provide dedicated dashboard for event correlation which should highlight all requests illegal or illegal of a particular attacker's session. Solution should also provide a security event	

	timeline dashboard, where critical events like Audit logs, Pool status change, Failover status change, DOS attacks, bug tracker option etc.	
4	Solution should have role-based management with multi factor user authentication, predefined roles/permissions configurations to manage who can see applications dashboard, edit and deploy services/policies for applications delivery and security, modify web application profiles etc. Roles can be associated with local users and groups, or users and groups from LDAP servers.	
5	Solution should also provide traffic performance statistics such as Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections etc.	
6	Solution should come with the system health monitoring capabilities to provide real-time awareness of the health of all the elements in the solution. The health monitoring should include alerts/alarm for Redundancy & High availability, Load and capacity, Network connectivity, Hardware etc. problems	
G	**Learning mode, transparent mode and AI/ML capabilities**	
1	Solution should support both a positive security model approach (A positive security model states what input and behaviour 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.	
2	Solution should provide facility to configure staging of policy, policy should move to blocking once staging time is over. It should also support configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection\learning mode.	
3	Solution should have fine tuning capabilities such as tracking unused elements in the policy and suggesting to remove them after a specified period of time.	
4	Solution should support regular expressions/ should support user-written scripts for the following purposes: Signatures definition, Sensitive data definition, Parameter type definition, Host names and URL prefixes definition, Fine tuning of parameters that are dynamically learnt from the web application profile etc.	
H	**Threat Intelligence Capabilities**	
1	The solution should have support for threat intelligence to identify new attack vectors. It should gather suspicious web requests, validate if the request are attacks and transform identified attacks into signatures. OEM should provide regular signature updates for threat intelligence and anti-bot signatures.	

2	The proposed WAF Solution should have real-time threat intelligence on known malicious IP sources, such as Malicious IP Addresses, IP Geo-location, Phishing URLs etc	
3	The proposed OEM should disclose Common Vulnerabilities and Exposures (CVEs) periodically	
I	**BOT and DDOS capabilities**	
1	Solution should have advanced BOT detection mechanism based on smart combination of signature-based and heuristic behaviour analysis techniques like client behavioural analysis, server performance monitoring to accurately distinguish traffic between human /bot traffic, identify “good” and “bad” & "suspicious" bots, and escalate using JavaScript, Image and sound CAPTCHA challenges.	
2	Should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioural analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.	
3	Solution should have ability to dynamically generate signatures for L7 DoS attacks.	
S. N.	**Desirable Features**	**Marks**
1	The proposed solution should offer load balancing functionality. If the solution has multiple modules they should be offered from the same OS version (e.g WAF, Load balancing etc).	10
2	Solution should have ability of HTTP response logging	10
3	Solution should also have the capability to highlight only malicious payload in any colour code from the entire attack payload on the event analysis dashboard for detailed forensics analysis.	10
4	Solution should offer protection for FTP, SFTP and SMTP protocols.	20
5	Solution should be able to dynamically create L4/L7 services on LB systems and load balance network traffic across the services via Monitoring the orchestration API server. The service should be able to modify the LB system configuration based on changes made to containerized applications. The service should support Kubernetes or Open Shift either CLI/API.	10
6	Whenever WAF detects an attack, it should also provide CVE number for that attack vector in order for security team to understand the vulnerability exposure	10
7	Solution should have a feature to generate device snapshot reports that can be used to get feedback on the health of the unit, missing hotfixes and best practices from OEM.	10
8	Solution must allow re-learning of an application profile on a per-URL or per-page basis and it should not be required to relearn the entire application. It should also have policy roll-back mechanism.	10
9	Should provide the ability to apply the following actions against traffic classified as BOT: (2 marks each) · blocking · monitoring	10

	· displaying a captcha · identify · delay	

E. DMZ Server Load Balancer (SLB)

	Server Load Balancer (SLB)	
Sr. No.	**Mandatory Features**	**Compliance (Y/N)**
1	The solution should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy.	
2	Highest level of OEM enabled Support is required for Software & Hardware.	
3	High availability should be achieved using same make/model license and same production licenses. There should not be use of any UAT/test license on secondary device, both licenses should be production grade with all the functionalities. Proposed solution should work in Active-Active mode.	
4	The appliance should be purpose built hardware	
5	The proposed appliance should support the creation of multiple vADCs, each with the capability to enable or disable Crypto/Compression Acceleration. When enabled, the vADC will leverage hardware for SSL/TLS encryption and compression offloading. If disabled, all encryption and compression processes will be handled by software.	
6	The proposed appliance should allow to disable root and bash access to the vADC for security purposes	
7	The proposed appliance for webUI and API should use a token-based authentication and timeout is based on five token refreshes failing. This is essential for security of the devices	
8	The proposed OEM should disclose Common Vulnerabilities and Exposures (CVEs) in Quarterly Security Notifications (QSNs). The OEM should also supply an online portal to run system diagnostics. The online portal should allow for PDF export of health report of the device highlighting CVEs affecting all modules of the device and their fixes	
9	The online health portal should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	
10	The online health portal should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes and EOS dates	
11	The appliance should be a full proxy architecture and should also be capable of performing as explicit proxy to fwd traffic generated by servers to internet	

12	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1	
13	The proposed solution should have minimum 8x10G/25G ports and 2x40G/100G ports from day1. The proposed solution should support conversion of same above ports to 8*25G in future if required.	
14	The solution should be supplied rack mountable and support rails if required.	
15	The solution should be supplied with console port and dedicated out-of-band management port	
16	Memory and OS assigned per instance. Each virtual instance should be able to work independently in high availability on same hardware pair. This should not compromise performance and efficacy of solution.	
17	The appliance should support the layer 7 throughput should be at least 55 Gbps scalable to 90 Gbps on same hardware with license upgrade. (Data references for above should be verified from publicly available datasheet)	
18	The proposed appliance must have minimum hardware compression of 30 Gbps for HTTP traffic form day 1 and scalable upto 45 Gbps with add on license on same hardware. (Data references for above should be verified from publicly available datasheet)	
19	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 30 Gbps Scalable upto 45 Gbps on same hardware with license upgrade.	
20	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data references for above should be verified from publicly available datasheet with SSL)	
21	The proposed appliance should support minimum 70 million L4 concurrent connections from day one and scalable upto 90 Million on same hardware with license upgrade.	
22	The proposed appliance should support minimum 2 million L7 requests per seconds from day 1 and scalable upto 4 million on same hardware with license upgrade.	

23	The solution must have TLSv1.1 and TLSv1.2 and TLSv1.3 on both client and server side and future release.	
24	The solution must have application-level load balancing including the ability to act as HTTP 2.0 Proxy.	
25	The solution must have full proxy architecture with HTTP Keep-Alive to allow the load balancer system to minimize the number of server-side TCP connections by making existing connections available for reuse by other clients for TCP optimization.	
26	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers.	
27	The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.	
28	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.	
29	To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user.	
30	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, HTTP Compression, caching etc. in active-passive mode. All the features should be enabled in Full-Proxy Mode.	
31	The proposed solution without any scripting should natively be able to support L3/L7 policies which can match conditions like Client SSL details, CPU usage, Geo IP, value in HTTP headers like cookie, auth, user-agent and tcp based information to enable/disable security features, HTTP profiles, SSL profiles, compression, caching etc. The system should also provide statistics around these policies in GUi where details like invoked and success rates are mentioned	
32	The proposed solution should be able to customise TCP behaviour for client side as well as server-side traffic for optimising of application. The proposed solution should provide timer management for TCP like close wait, Fin wait 1, fin wait 2, idel timeout and should also provide an option for sending proactive	

	RST packets when a session is timeout to make sure stale connections are cleared immediately.	
33	The proposed solution should be able to define the memory management for TCP connections where send buffer, receive window values in bytes should be configurable	
34	The proposed solution should be able to full proxy a tcp connection between the client and server, while also making sure it only completes a client side tcp handshake only if the server is responding to SYN packets with ACK. This should be configurable parameters to make sure if the server side is not responding to connections the client-side connections does not receive an ACK	
35	The proposed solution should also allow for congestion control mechanism/options like Appropriate Byte Counting (RFC 3465) , slow start & Timestamps Extension for High Performance (RFC 1323)	
36	The proposed solution should also provide loss detection and recovery mechanism/options like D-SACK (RFC 2883) , Maximum Segment Retransmissions & Maximum Syn Retransmissions	
37	The proposed solution should also provide static and dynamic bandwidth control at each virtual server level. The max rate should be definable in bps, kbps, mbps and gbps. The solution should also be able to specifies the maximum amount of bandwidth that each session associated with the bandwidth control policy can use in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps). The solution should also be able to define a PPS based limit, where the user can define the rate in packets per second (PPS), kilo packets per second (KPPS), mega packets per second (MPPS), or giga packets per second (GPPS) this is helpful as DoS limiter	
38	The proposed solution should also support QUIC protocol with option of setting the Bidirectional Concurrent Streams Per Connection & Unidirectional Concurrent Streams Per Connection	
39	The proposed solution should support HTTP/3 with an option to specify the max header table size.	
40	The proposed solution should also support HTTP2 with options to define and customise Concurrent Streams Per Connection , Connection Idle Timeout , Insert Header with custom name, Enforce TLS Requirements with support for ALPN mode of activation. The solution should support an option to specify the max header table size. The HTTP2 protocol compresses HTTP	

	headers to save bandwidth. A larger table size allows better compression but requires more memory.	
41	The Solution should have IPSEC tunnelling capabilities	
42	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Diameter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts	
43	The proposed system should allow to set a delay in the marking of a pool member or node as up for some number of seconds after receipt of the first correct response. The purpose of this feature is to ensure that the monitor marks the pool member or node as up only after the pool member or node has consistently responded correctly to the LB system during the defined time period.	
44	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Diameter and MQTT traffic	
45	The proposed solution should be able to host multiple backend applications on single Virtual IP and should be capable to identify SNI value to make a forwarding decision	
46	The proposed solution should support nodes	
47	The proposed solution should support dynamically create L4/L7 services on LB systems and load balance network traffic across the services via Monitoring the orchestration API server, the service should be able to modify the LB system configuration based on changes made to containerized applications.	
48	Native support for Geolocation data base without need of additional licenses	
49	System should support Standard HTTP, Explicit HTTP, and Transparent HTTP profiles natively without need of scripting	
50	Load balancer should support creation of Virtual servers which can be categorically offloaded to hardware chipsets. The level of offload to chipset function should also be customizable.	
51	It should be possible to set Send and Receive buffers manually as well as system should be intelligent enough to tune the buffers automatically to give optimum performance of application access.	
52	The proposed solution should support native integration with containerized platforms hosting microservices e.g. OpenShift, TKG cluster etc. Solution should update the	

	configuration of LB automatically by observing events within clusters form day 1 without add on license.	
53	The proposed solutions Stateful Session Failover's should be supported between minimum 6 Units if required to support infra growth.	
54	The proposed solutions Stateful Session Failover's cluster must support latest TLS 1.3 Ciphers. The proposed solutions Stateful Session Failover's cluster must support communication between appliances and real servers over SSL (SSL real host)	
55	The proposed solutions Stateful Session Failover's cluster must support Header insertion, compression, cache, HTTP/2, ePolicy, TCP Selective Acknowledgment (SACK) function on per VIP basis	
56	The proposed solution should have nomenclature flexibility to name and the real service and virtual service identical names	
57	The proposed solution should support HTTP/2 real service group persistence based on a string obtained from the request body	
58	The proposed solution should be able to configure a virtual service IP which is already a part of interface IP.	
59	The proposed solution must allow SNAT to be configured for std protocols but also for RTSP, PPTP, SOCKS etc	
60	The proposed appliance must allow the creation of wildcard 0.0.0.0 service for SSL traffic, without the need for enabling SSL interception to passthrough traffic transparently independent of protocol.	
61	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establish a secure tunnel with authentication against AD/OAUTH/Radius and MFA.	
62	The proposed solution must offer out of band programming for control plane along with data plane scripting for functional like content inspection and traffic management	
63	Server Load Balancer should support SQL-based querying for the following databases for health checks: for Oracle, MSSQL, MySQL, PostgreSQL and other databases if required in future	
64	Proposed solution should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover for all connections which are offloaded on the device so that existing SSL connections are not lost during a failover event	
65	The proposed appliance should support centralized Security policies enforcement, SSL Certificates management for workloads on Private DC and public cloud	

66	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration. Further it should also provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc.	
67	Device should support netflow and SIEM integration.	
68	Solution should support mirroring of connection and persistence information to peer device to avoid service impact during failover	
	a. Web servers	
	b. LDAP servers	
	c. Email servers	
	d. RADIUS servers	
Sr. No.	**Desirable Features**	**Marks**
1	The proposed solution should be capable to provide add-on modules and services on the same hardware like WAF, Zero Trust app access, OAUTH integration, DNS with Security and SSL VPN with add-on licenses if required in future	10
2	The solution must support automatic or manual updation of certificate bundles of CA installed on it to reduce administrative workload and simply SSL certificate management.	10
3	The solution must support Constrained Certificate delegation which will allow the device to generate SSL certificates on behalf of the application servers which then can be used to authenticate clients for which SSL certificate-based authentication has been enabled.	10
4	Should Support integration with SIEM and other Monitoring and Reporting solution	10
5	Device should be able to provide compliance reports.	10
6	The solution should allow combining multiple monitors to create monitor groups.	10
7	The solution should support monitoring of the Load Balancer via SNMP.	10
8	The solution should have a web-based administration.	10
9	Device should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	10
10	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	10

F. Perimeter SSL Orchestrator:

	SSL Orchestrator (SSLO)	
Sr. No.	**Mandatory Features**	**Compliance (Y/N)**
A	**Solution Deployment and Compatibility**	
1	Device should be based on dedicated hardware appliance. The platform should have a minimum of 4x100G/40G (for connectivity with both Intranet and Internet switches), 16x25G/10G ports. It shall be populated with atleast 16x10G and 4x40 G from day 1.	
2	The SSL solution device shall be able to support inline bridge mode, decrypt/encrypt SSL traffic without change the SRC/DST IPs and network IP segment topology and various configuration topologies such as Outbound transparent proxy, Outbound explicit proxy, Inbound reverse proxy, Outbound layer 2 and Inbound layer 2.	
3	The SSL Offloader device should be able to support proxy chaining and act as a explicit forward proxy and authentication mechanisms such as Explicit forward proxy authentication, Transparent forward proxy authentication (captive portal), authentication with NTLM and Kerberos, delegate token authentication offload,	
4	Should support minimum SSL Visibility TPS : - 380 K TPS (RSA 2k keys) from day 1 - 280K TPS (ECDHE-ECDSA P-256) from day 1	
5	The SSL Solution should support minimum SSL connections : - L7 requests per second: 10 M - L4 connections per second: 3 M - L4 concurrent connections: 390 M	
6	The SSL Off loader must have minimum 72 vCPUs Memory: 512 GB Storage: 2X 2 TB SSD	
7	The Solution should support active-active configuration for incoming traffic. Traffic to incoming applications will be split across the proposed solution with one application being active on one unit.	
B	**Hardware requirements**	
1	The proposed solution should have atleast 100 Gbps bulk SSL encryption capabilities.	
2	Solution should support hot-swappable fan and dual Power supply for redundancy.	
C	**Decryption capabilities**	
1	Solution should have capabilities to perform selective tool bypass during SSL/TLS decryption, enabling bypass based on the following conditions:	
	a. SSL decrypted traffic	
	b. Non-decrypted SSL traffic (non-SSL TCP)	

	c. Non-SSL traffic (non-TCP)	
2	Solution should support decryption policies and traffic segregation that will be based on specified whitelisted and blacklisted domain, hostname functionality, URL categorization, Application type, MAC addresses, IPv4/IPv6 addresses, VLAN ID, VXLAN ID or a User Defined Attribute (UDA) etc.	
3	Solution should have the ability to import server side certificates and private keys for decryption and multiple self-signed internal (organizational) or external CA's and PKI structures	
4	Solution should allow SNAT to be configured for std protocols but also for RTSP, PPTP, SOCKS etc	
5	Solution should allow the creation of wildcard 0.0.0.0 service for SSL traffic, without the need for enabling SSL interception to passthrough traffic transparently independent of protocol.	
6	Solution should intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	
7	For outbound, the SSL device shall use the same SSL version and SNI options as client, re-encrypt application data, which may be modified by the external security devices (such as WAF, DLP) to the original destination.	
8	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. Should support OCSP protocol to check the validity of the certificates online, Certificate bases access control, CRL's (HTTP, FTP, and LDAP) etc.	
D	**Service chaining capabilities**	
1	Solution should have the ability to service chain. The solution should decrypt the SSL traffic and send specific decrypted traffic to selective security solutions as defined. Solution should have the ability to insert or delete security solutions in the service chain.	
2	Solution should support configurable weighted load sharing across multiple similar inline and/or monitoring security devices to support active-active high availability mode.	
3	Solution should support N+1 and 1+1 inline tool redundancy for inline tools along with health probes to decide failover actions.	
E	**Integration Capabilities**	
1	Solution should integrate with Enterprise level SIEM solution, NTA solution, SOAR solution and any other solution part of this RFP or decided by the bank.	
2	Solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of target service automatically by observing events within kubernetes clusters.	

3	Solution should be able to configure a virtual service IP which is already a part of interface IP.	
F	**Dashboard, user management and troubleshooting capabilities**	
1	Solutions should have extensive troubleshooting capabilities to collect packet captures, debugs endpoint, to generate SSL related events logs such as Ingress/Egress VLAN, policy rule names, URL categories, TLS handshake status, reset causes, and connection failures etc.	
2	Should support SNMP v2 & v3 traps, email alerts and SNTP/ NTP. Device should send SNMP traps to centralized server and should provide login/ logout, configuration changes, dumps information.	
3	Solution should support authentication via local databases, LDAP, Active Directory, RADIUS, TACACS+, certificates, SAML, OAuth, Kerberos, and two-factor authentication for enhanced security.	
4	Solution should have mechanism that lets you create a backup copy of your deployed configurations	
5	Solution should provide a rich set of methods based on context to dynamically determine how best to optimize the flow through the security stack. Context can minimally come from artifacts such as Source IP/subnet, Destination IP/subnet, IP intelligence category, IP geolocation, Host and domain name, URL filtering category, Destination port and protocol etc.	
6	The solution should have the capabilities to support role-based access control to manage configuration and monitoring operation, by providing different groups of users with different level of access	
G	**Threat Intelligence/Security Capabilities**	
1	Solution should identify and prevent the known TLS exploits & vulnerability like Heartbleed and reset the tcp connection.	
2	The SSLO device should be able to also perform URL Filtering, IP intelligence, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicit proxy) functionality. It should also provide zero trust checks for clients trying to access applications protected by SSL Offloader.	
3	Solution should support Extended Validation (EV) certificates	
H	**Other technical capabilities**	
1	The SSL Offloader device should have flexible ICAP request or respond policies, such as enabling ICAP only for HTTP response , only for HTTP POST , for specific request URL extensions and response content types	
2	Solution should provide the ability to test for a valid server-side connection before completing the client-side handshake. The system sends the server a SYN cookie before responding	

	to the client's SYN and verifies that the pool member is available to accept the connection.	
3	Solution should support SSL termination with TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0 protocols and should be able to detect and decrypt all TCP ports that utilize SSL/TLS (TCPS) communication.	
4	The solution should support secured RESTful API or XML-RPC for simple 3rd party remote management. The SSL Interception device shall support secured WebUI (HTTPS) access.	
Sr. No.	**Desirable Features**	**Marks**
1	The proposed hardware should support dual SSL chipset for better resiliency and availability	10
2	Solution should intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS) eg. SFTP, IMAPs, POP3S etc. and support port forwarding (transparent and non-transparent) for FTP and other protocols.	20
3	Solution should provide certificate vault feature along with security features such certificate encryption, restriction on certificate modification etc.	5
4	Solution should provide the ability to SSL profile switching based on Client Hello SNI matches. (functionality required to host multiple API servers on single VIP)	5
5	Solution should be able to decide based on parameters (such as client IP, destination port, etc) to enable TCP keep-alive and ability to support decryption of mTLS traffic without the need for client's end certificate	20
6	Solution should have the ability to matching traffic based on incoming database group value for Server Name (TLS ClientHello)	10
7	Solution should detect DNS-over-HTTPS traffic	10
8	The SSL Offloader devices should have the ability to support C3D.	10
9	The SSL Offloader device should provide the ability to include an authorityKeyIdentifier (AKI) in the forged server certificate to aid in certificate path discovery at the client. Path discovery is the mechanism that a TLS client performs to find and build a complete chain of trust from the end-entity (leaf) certificate to the explicitly trusted root CA.	5
10.	The solution should support NIST-standardized Post-Quantum Cryptography (PQC) algorithms and provide cryptographic agility to adopt future updates to these standards	5

G. Global Server / Link Load Balancer:

	Global Server Load Balancing (GSLB) & DNS security & Link Load Balancer	
	Mandatory Features	**Compliance (Y/N)**
1	The solution should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy. The proposed solution should offer recursive DNS and Auth DNS feature and protections around the same from Day-1	
2	Highest level of OEM enabled Support is required for Software & Hardware.	
3	For Hardware: Guaranteed 4 Hour SLA with (24*7*365 x4hrs) for the failed Hardware parts.	
4	Proposed GSLB solution should have capabilities to create IPSec tunnel on the same device from day1.	
5	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1	
6	The proposed solution should have minimum 8x10G/25G ports and 2x40G/100G ports from day1. The proposed solution should support conversion of same above ports to 8*25G in future if required.	
7	The solution should be supplied rack mountable and support rails if required.	
8	The solution should be supplied with console port and dedicated out-of-band management port	
9	Memory and OS assigned per instance. Each virtual instance should be able to work independently in high availability on same hardware pair. This should not compromise performance and efficacy of solution.	
10	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data references for above should be verified from publicly available datasheet)	
11	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data references for above should be verified from publicly available datasheet)	

12	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based processor for acceleration) (Data references for above should be verified from publicly available datasheet)	
13	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data references for above should be verified from publicly available datasheet with SSL)	
14	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.	
15	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with license upgrade.	
16	The solution must have TLSv1.1 and TLSv1.2 and TLSv1.3 on both client and server side and future release.	
17	The appliance should have Global Load Balancing feature from day 1	
18	System shall be performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery	
19	System should have global response time optimization in real-time through advanced load and response-time measurements	
20	The appliance shall have failover capability between data centers in active-active or active-backup modes	
21	The appliance shall perform global redirection based on DNS	
22	The appliance shall perform global redirection based on HTTP redirection	
23	The appliance shall support delegating a sub domain that handles all DNS requests for geographically load balanced servers/VIPs	
24	Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS & A, AAAA, MX, and NS queries as External DNS	
25	The appliance shall support secure DNS resolution for A, AAAA, PTR, SOA records (DNSsec)	
26	The appliance shall support returning multiple addresses when resolving a domain name	

27	The appliance shall support user configurable network/ end-user geographical location based rules with DNS to server mapping	
28	The appliance shall integrate global load balancer solution with the server load balancing solution in order to effectively gauge site-to-site load distribution.	
29	The appliance shall support the grouping of multiple DNS servers together for the purposes of persistency.	
30	Able to secure synchronize configurations, DNS configuration, and persistence to provide stateful-failover of DNS query	
31	Able to autosync setup and synchronization of multiple devices thus eliminating difficult hierarchical management common to DNS	
32	Provides global high availability and reliability of applications across multiple sites and ensures application availability by tracking and managing interdependencies between applications.	
33	Shall have a GUI integrated zone file management tool that simplifies DNS zone file management and reduce the risk of misconfiguration. It shall provide a secure environment to manage DNS infrastructure while validating and error-checking zone files.	
34	Shall perform multiple firmware and firmware uploads without resetting device	
35	Able to cache DNS responses	
36	Able to provide flexibility in having deterministic probers which communicate with each node to determine (depending on the probe or monitor configured) its availability, status, proximity, or responsiveness.	
37	Able to perform intelligent probing of your network resources to determine whether the resources are up or down. This allows you to specify which device probe specific servers for health and performance data.	
38	Able to inform administrator of query stats of device groups in synchronisation to improve visibility, management and troubleshooting of groups	
39	Able to support composite monitors, such as M of N rule (eg. need only 2 successes out of 3 monitors).	
40	Able to support static and dynamic load-balancing algorithms such as :	
	· Round robin	
	· Global availability	
	· LDNS persistence	
	· Application availability	
	· Geography	
	· Virtual server capacity	
	· Least connections	
	· Packets per second	

	· Round trip time	
	· Hops	
	· Packet completion rate	
	· User-defined QoS	
	· Dynamic ratio for Member/Node	
	· Observed Node/Member	
	· Ratio	
	· Kilobytes per second	
	· RADIUS accounting	
	· Member/Node Ratio	
	· Fastest Node	
	· Weighted Least Connection on member/node	
	· Predictive Node/Member	
41	Supports built-in GEO-Location database for accurate geo load balancing. The default database shall provide geolocation data for IPv4 addresses at the continent, country, state, based on IP Address available. This also allows user to define how traffic is routed based on this information.	
42	Support intelligent routing with load balancing geography based distribution via programmatic control	
43	The proposed solution should able to support application-centric monitoring, persist user connections across applications and data centers and be automatically routed to the appropriate data center or server, based on application state, ensuring that users are directed back to the same site regardless of their entry point.	
44	The proposed solution should able to propagate the desired persistence information to local DNS servers, reducing the required frequency of synchronizing back-end databases and maintain session integrity.	
45	Supports DNS fallback in case GLSB decision is not available	
46	Deliver high speed standard (non-GSLB) DNS query responses. E.g. addressing queries at very high speed by obtaining configuration via zone transfer from primary authorative DNS Servers and accommodate large numbers of zones and records in range of tens of millions	
47	Support scripting languages that have the ability to manipulate and control traffic passing through the controller	
48	The proposed solution should be able to define and control how traffic is distributed across links, based on real-time traffic flows and throughput	
49	Support IPv6	
50	The solution shall be able to provide load-aware DNS resolution with SNMP and scripted health monitoring for tracking cpu consumption of application resources for which dns resolution is needed.	

51	The proposed solution should be able to handle high performance logging for all DNS critical functions	
52	The proposed solution should be able to increase the query of data and information with high-speed logging (unified logging) of DNS queries and responses enabling fast recognition of queries for quick searching and displaying	
53	The proposed solution should be able to provide comprehensive DNS detail statistics such as query type (A, CNAME, NS, RRSIG, AAAA, SRV and "other" types) with Request/Percentage plus Response/Percentage counts.	
54	The proposed solution should be able to check statistics in profile and in analytics module. Giving comprehensive DNS statistics in graphical format	
55	The proposed solution should be able to provide Advanced DNS Analysis and Reporting of Applications, virtual servers, query name, query type, client Ips, top requested name, 2nd level domains, LDNS Ips etc	
56	The DNS solution should support the functionality of clustering two devices so as to ensure a highly available, high performance DNS service on a single IP address	
57	The DNS solution should support synchronize the configuration files and zone files to ensure that any update to the configuration will be populated between systems of the solution	
58	The DNS must support DNS64 functionality as per RFC 6147	
59	System should support for:	
	a. Flushing the live cache without restarting the server	
	b. Specific portions of the cache can be discarded without restarting the server	
	c. Optimised memory management for caching as per traffic load	
60	The DNS system should support updation of:	
	a. DNS records TTL	
	b. Zone email servers-MX records	
	c. Zone DNS servers-NS and SOA records	
	d. Primary IP addresses for secondary zones	
	e. Reverse DNS records (A/AAAA record modified)	
61	DNS System should support for authoritative DNS requirements:	
	a. Managed BIND resolver, with support for TSIG and IP secured zone transfers	
	b. Delete zones, force updates, display zone files	
	c. Full support for DNSSEC signed zones	
	d. Compatible with any standards-compliant DNS server	
62	DNS System should support for DNS Cache Requirements	
	a. High performance recursive resolver with support for forward zones and global forwarding	
	b. Optimised DNSSEC validation	

	c. Cache poisoning protection – max randomness for query ID and port, case preservation, response scrubbing, access control	
63	The DNS system should be able to isolate services such as recursive and authoritative resolution and traffic to DNS system onto different IP addresses and multiple NICS	
64	The DNS system should support for TSIG keys to secure connections between Internal DNS and 3rd party DNS servers	
65	The DNS system should provide an authoritative DNS service mitigating the risk of cache poisoning and denial-of-service attacks by leveraging a number of technologies, including IP Any-cast, secured zone transfers, router-protected name servers, and non-BIND-based DNS to provide a highly secure and fault-tolerant DNS service	
66	The DNS system should facilitate Incremental zone transfer (IXFR)- support IXFR protocol - transfer only changed data, instead of having to transfer the entire zone as per RFC 1995 and 5936	
67	The DNS should support for data validation while inserting data during DNS configuration	
68	The DNS solution should support Non-Terminal DNS Name Redirection as per RFC2672	
69	The DNS solution should support xNAME RCODE and Status Bits Clarification as per RFC6604	
70	Must be an hardware appliance with propritery and hardened OS.	
71	Must be intelligent DNS which can check health of server and resolve based on Availability of server at Primary Datacenter or Secondary Datacenter	
72	The offered solution should provide DNS Firewall functionality by detection and mitigation of DNS reflection or amplification DDoS attacks, DNS Flood, protocol violations, bad request types attacks and other DNS threats and functionality includes the following: • Protocol inspection and validation • DNS record type ACL • High-performance authoritative DNS, which scales responses exponentially • Authoritative DNS hyper scaling up to 200 percent to absorb DDoS attacks • Reducing latency and hyper scaling DNS caching • DNS load balancing • Stateful inspection (never accepts unsolicited responses) • The ability to scale across devices using IP Anycast • Secure responses (DNSSEC) • DNSSEC response rate limits • Complete DNS control using DNS event driven programming • DDoS threshold alerting • Threat mitigation by blocking access to malicious IP domains	

	• DNS logging and reporting • Hardened DNS code (not BIND protocol)	
73	Solution shall have access control lists (ACLs) for queries and recursive queries. The solution should support time schedule-based access control list.	
74	The DNS must have security features such as configuration of ACL (Access Control Lists) and named ACL	
75	The DNS system solution should have DNS Firewall functionality	
76	Should shall have Security features from day 1	
	a. DNS DOS/DDoS attack, LAND Attack etc.	
	b. DNS Malware Protection	
	c. DNS Botnet Protection	
	d. DNS reflection Attacks	
	e. DNS Amplifications Attacks	
	f. DNS Tunnelling Attacks	
	g. DNS Based exploits	
	h. TCP/UDP/ICMP Floods	
	i. DNS Protocol Anomalies	
	j. Reconnaissance based attacks	
77	Should perform Hyper-scale Service Responses and Absorb DNS DDoS . Hardware Acceleration for DNS Caching	
78	The solution must detect and mitigate all known DDoS attacks in general from L3 till L7	
79	The solution must detect DDoS attacks based on signature using inbuilt IPS engine with support for dynamic updates and mitigation should support rate limiting with CPTCHA challenge or request blocking. The IPS engine should also allow creation of custom signature using snort filters.	

80	Should also have support in future with additional license: 1) DNS filtering 2) DNS query limit 3) Automatic detection of DNS flood	
81	System should support failover to reduce failover time less than 5 second with all sessions persistence.	
82	System should support network-based failover for session mirroring, connection mirroring and heartbeat check	
83	The Active DNS server must notify the standby DNS to update the records in real time in case any change happens in zone files located on active server.	
84	Solution should support of high-availability (HA) and port resiliency (NIC Failover) in each appliance	
85	System should support all functionality when configured in a HA pair and should support for Data synchronization provided for all protocols and services served by devices	
86	The solution should support link failure detection with support for upstream router or object tracking starting from physical level checks to ICMP/TCP probes to check path availability.	
87	The solution should support hitless stateful failover between devices/virtual instances in a cluster in case of failures with help of session synchronization	
88	The systems should provide SSH and HTTPS interface management for administering the device	
89	The system should support for local logging for 30 days	
90	The system should support for configuring multiple external Syslog servers including severity of messages for sending logs and should get synchronised with external DNS and NTP systems	
91	The system should support for monitor and manage using 3rd party Network Management System/Element Management System (NMS/EMS) software using SNMP and SNMP V.3	
92	The device should be able to capture Device related stats in tcpdump packets.	
93	Must have feature to mask, omit and manipulate the data/fields being sent to log server over syslog.	
	Desirable Features	**Marks**
1	The proposed solution should be capable to provide add-on modules and services from the same hardware like WAF, Zero Trust app access, OAUTH integration, DNS with Security and SSL VPN with add-on licenses if required in future	5
2	The appliance shall support the availability status of any VIPs using standard health monitors	5
3	The proposed solution should be able to provide statistics per profile and per device global count	5
4	The proposed solution should be able to provide manual GSLB configuration copy. This scalability feature for large configuration with rapid user changes can be saved manually.	5

5	The proposed solution should be able to view Cache Hit, Cache Miss Ratio	5
6	The DNS should have the capability to be configured as authoritative and caching DNS	5
7	The Solution should have real time distributed database management with all DNS appliances	5
8	The DNS solution should provide appropriate automated failover and disaster recovery mechanisms	5
9	The DNS solution should support synchronization of all devices via a shared distributed database	5
10	The solution should use standard encrypted protocol for communications between the devices	5
11	The DNS solution should support both types of query mechanism: Recursive and Iterative	5
12	System should support transparent failover between 2 devices, the failover should be transparent to other networking devices.	5
13	The system supports different account management features for local administration like:	
	a. addition, deletion and modification of a user account	2
	b. The account password, operation limit and operation privilege can be set and modified	2
	c. The operation limit specifies the lifetime of a user account	2
	d. The operation privilege specifies the scope of command groups that can be executed by the user	2
14	The DNS system should support:	
	a. Audit logging	2
	b. DNS query and response logging	2
	c. Syslog (Central loggin system)	2
	d. DNS debugging as per RFC 1713	2
15	The system should be able to set Password strength, password change frequency and can be enforced	5
16	The system should provide the following configuration management functions:	
	a. Setting of DNS parameters	1
	b. Configuration of Primary and Secondary DNS if any	1
	c. Configuration of Zones	1
	d. Configuration of Resource Records	1
	e. Configuration of the domain name resolution view	1
17	The system must provide the following web dashboard that should provide the following information related to system maintenance and management functions:	
	a. Process management (CPU and Memory Usage etc.)	2
	b. Configuration check	2
	c. Configuration saving	2
	d. Domain name test	1
	e. Performance statistics query	1
	f. Server running status query	1

18	The provided DNS solution should support DoT (Dns over TLS) or DoH (DNS over Https) functionality	5

H. Perimeter DDoS:

Sl No	Mandatory Features	Compliance (Y/N)
1	System should have Stateless appliances in DC and DR.	
2	Solution should have Fail-Open and Fail-Closed options for Hardware and Software Bypass feature to achieve faster network convergence in High Availability/Resilient Deployment.	
3	Proposed appliance must be purpose-built DDoS prevention system and not having any kind of state limitation such as TCP connections etc.	
4	Proposed appliance should be a dedicated appliance-based solution (not a part of Router, UTM, Application Delivery Controller, IPS, Load Balancer, Proxy based architecture or any Stateful Device)	
5	System should have scalable inspection throughput license approach capacity of 5 Gbps on Day 1. It shall be scalable upto 10 Gbps without additional hardware whenever needed.	
6	Proposed appliance should support DDoS Flood Attack Prevention Rate of atleast 25 million packet per seconds on the same appliance.	
7	System should mitigate encrypted attacks and should support minimum 60,000 SSL CPS measured with 2048-bit key.	
8	Solution should provide protection for volumetric/Protocol and Application layer-based DDoS attacks.	
9	Solution should be transparent bridge to pass 802.1 Q tagged frames and other control protocols like VLAN.	
10	In inline mode system must not modify MAC or IP addresses of passed frames.	
11	Solution should inspect, detect and mitigate IPV4 & IPv6 Attacks.	
12	System should prevent malware propagation attacks.	
13	System should support Multiple Segment protection for up to 6 Segments	
14	The device operating system should be hardened, and the responsibility shall fall on OEM to ensure the same	
15	System should support, In-Line, Out-of-Path deployments modes from day 1	
16	The system should support deployment on a “logical link bundle” interface through Link aggregation protocols like LACP	
17	DDoS Mitigation System should support Symmetric and Asymmetric Traffic flows	

18	Solution should be deployed with High availability/Redundancy architecture.	
19	Device should be fully integrated with an organization's existing security stack using REST API, SNMP, Syslog and STIX/TAXII	
20	System should have 8 x 10G Fibre protection ports and 4 x 1G Copper protection ports populated (from day 1) with multi-mode transceiver. All transceivers should be provided from day one. The 10 G ports should support 1 G transceivers also. Total number of transceivers required - 8 x 10 G and 8 x 1 G. It should be field replaceable.	
21	Should have dual redundant Hot-Swappable AC power supplies from day one	
22	Devices must be rack-mountable in standard 42U Rack	
23	System should support Bypass Capable NIC in combination of 1G (Copper/Fiber - SX/LX), 10G (SR/LR)	
24	Should have ready REST API for integration/ Anti-DDoS system for attack mitigation in custom portal	
25	Integration with RADIUS and TACACS+	
26	Device should integrate with Bank's existing SIEM engine seamlessly through Syslog messages, Network performance & monitoring solution, SOAR.	
27	Solution should support SNMP v2/v3 MIB and Traps	
28	System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability	
29	Proposed solution should have GUI based monitoring, configuration management, diagnostics and reporting.	
30	The system must have a dedicated management port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic.	
31	System should have CLI access over console port and SSH	
32	Solution should have Configuration and Login Audit trails	
33	Solution should support Role/User Based Access Control and reporting functionality.	
34	OEM to provide support in real-time to Bank during malware outbreak, DDoS attacks to identify and mitigate attack	
35	In case of DDOS Attack Bank should involve OEM to mitigate/ Optimise the traffic to safeguard the DataCenter	
36	Solution should provide DDoS attacks log backup and Filterable/Exportable Attack Log	
37	Solution should provide Email alerts and comprehensive reporting including on-demand, on-schedule in multiple formats	

38	Solution should be able to offer granular drill down reports based on hosts, sources, applications etc.	
39	Solution should provide the traffic statistics related to Application / Protocols.	
40	The solution shall provide real time dashboard displaying statistics on data such as total traffic, passed/blocked, top IPs/services/domains, attack types, top sources by IP location (Geo IP) and blocked sources, etc.	
41	DDoS Appliance must not have any limitations in handling the number of concurrent sessions for DDoS attack traffic.	
42	System has behavioural-based application-layer HTTP and HTTPS DDoS protection	
43	Should support user customizable/user defined Signature or Filters or Payload/Header based regular expressions	
44	System should allow to write manual ACL's to block IP's	
45	Solution must support searching for IPs which have matched IOCs/Blocked Hosts within last 10 days to understand if organisation was targeted	
46	System must have an In-Built updated IP reputation feed that has IOC for Active DDoS vectors, Botnets, etc. that are actively propagating DDoS attack vectors anywhere in the world. It should be automatically updated at a configurable interval to block and protect network against active attackers	
47	System should have options for Blacklist and Whitelist IP Address	
48	System should restrict the IP address from specific segment like from TOR network	
49	Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals	
50	The system should be capable to detect and mitigate both inbound and outbound attacks.	
51	Anti-DDoS Appliance should support Automated AI Analytics Engine, Behavioural Analysis, Challenge-response methods or Auto-Signature to detect and mitigate Zero day DoS, DDoS attacks	
52	Solution must support Machine Learning based Adaptive DDoS Protection that adapts to Dynamically Changing DDoS Attacks by automatically detecting new attack techniques and providing targeted mitigation	
53	The system must be able to block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and	

	provide statistics for the packets dropped. Solution should also support packet Anomaly Protection.	
54	System should protect from TCP Out-Of-State attacks.	
55	System should Protect from multiple attack vectors on different layers at the same time with combination OS, Network, Application, and Server-side attacks	
56	System should support suspension/dynamic suspension of traffic from offending source based on a signature detection, host behavioural analysis, malformed packets, payload expression matching	
57	The system must support Connection limit option to limit number of new connection on per source basis or in range or equivalent	
58	The system must allow Network Security policies to be changed while the policy is in active blocking/running mode and should not affect running network protection.	
59	Should detect and Mitigate attacks at Layer 3 to Layer 7.	
60	System should have counter measures & challenge response-based approach for immediate mitigation of flood attacks—protecting against unknown DDoS attacks without manual intervention. The system should not depend only on signatures for mitigation of DDoS attacks.	
61	System must be able to detect and mitigate Spoofed SYN Flood attacks and should support different mechanisms like: a) TCP Authentication b) TCP Out of Sequence Authentication c) HTTP Authentication - Redirect d) HTTP Authentication - soft reset e) HTTP Authentication - JavaScript	
62	System must be able to detect and block from Flood based attacks on Network and Applications like - TCP, UDP, ICMP, DNS, HTTP and HTTPS GET/POST Flood.	
63	System should Protect from Brute Force/reflection/dictionary & amplification attacks or equivalent	
64	System should be managed from Centralized console. Centralized Console should have capability to manage all the devices in terms of configuration, alerts and reporting.	
65	Centralized Console should give Attack Analysis detection and possible attack traffic. Also, should provide recommendations for mitigating any attacks that it detects.	
66	Centralized console should give consolidated DDoS historical and trending reports.	

67	System should detect and mitigate different categories of Network Attacks viz. Volume based, Protocol, Application attacks etc.	
68	System should be able to provide (Layer 4 to Layer 7) Challenge action apply to suspicious/all source	
69	Should detect and Mitigate from Low/Slow scanning attacks	
70	Solution should support blocking inbound scanning and known brute force attempts	
71	Solution should support mitigation of Burst Attacks using mechanisms like Rate-Based Blocking or Flexible Rate-based blocking, Signature or equivalent.	
72	The system must limit number of simultaneous TCP connections on a per-client basis	
73	Solution should support Automatic adaptive thresholds estimation for critical L3, L4 and L7 parameters	
74	System must be able to detect and block Zombie Floods	
75	System provides behavioural-DoS protection using real-time signatures, challenge/response mechanism	
76	The system must support the dropping of idle TCP sessions if client does not send a user-configurable amount of data within a configurable initial time period and should dynamically blacklist the offending sources.	
77	Should support IOC Types - IP Address or Fully Qualified Domain Names/URLs	
78	System protects from DDoS attacks behind a CDN by surgically blocking the real source IP address	
79	Solution should support SSL renegotiation & Cipher Anomalies Attack Mitigation	
80	System protects against SSL/TLS Encrypted DoS and DDoS threats both at the SSL/TLS Layer and HTTPS layer	
81	System should provide protection from known attack tools that attack vulnerabilities in the SSL layer itself with a separate SSL Decryption module on device or out of path	
82	Should have capability to identify malicious SSL traffic based on behaviour analysis, payload inspection	
83	Should protect against attacks that exploit SSL or TLS on application servers such as Web, Mail, or secure VPN servers	
Sl No	**Desirable Features**	**Marks**
1	The appliance should support Hardware and Software Bypass Capability with both fail open and fail closed modes in all protection ports (including Copper and Fiber). The hardware bypass for all protection interface types (Copper and Fiber) can be either In-Built in the Appliance or with an External hardware bypass switch	10

	from the same OEM as Anti-DDoS appliance which should also be provided.	
2	Should support latency less than 75 microseconds. Latency should be documented in datasheet	10
3	The proposed system shall do automatic cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation.	10
4	Should have support for blocking minimum 1 million IoC's inbuilt on the device and should support blocking at least 2 million IOCs via integration with 3rd Party Threat Intelligence Platform for the blocking of malicious traffic with STIX/TAXII.	10
5	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain IOC to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a configurable interval.	10
6	Solution should detect SSL encrypted attacks at Key size 2K without any hardware changes.	10
7	The management console should have scripts to automate common tasks on manage DDOS devices, includes the RBAC roles that are permitted to run the script	10
8	The management console should support export and import DDOS device configuration templates which include the configuration, security settings and/or baselines of a Protection policy	5
9	The management console must support REST API to view security events from DDOS devices	5
10	The device should support User Defined Feed enforcement for large scale IP or subnet blocking from an external file in CSV format, these external files can be manually loaded via device configuration or automatically using an API.	10
11	System should have native Integration with atleast three ISP or MSSP in India for Cloud-based mitigation.	10

Network Rack

S.no.	Technical Specifications
1	42U Network rack with minimum dimension (HDW) 2000mmX1200mmX1000mm. Colour - powder-coated black colour, RAL 7021 (80 - 120 MICRONS) with locks. The number of racks proposed should be sufficient to place devices/switches etc.
2	The design of the rack should be in accordance with the following agency standards or certifications. · EIA-310 standard for IT rail hole spacing. · CE Certified as per EN IEC 62368-1 /UL or UL Certified as per 60950-1 & UL 2416 · RoHS
3	All rack components door, side panel, top panel, 19” rail, PDU bracket shall be directly grounded to the frame to eliminate any external grounding wire and frame must have provision of grounding points to ground each rack to the building ground.
4	All 19” rails should be made of 14-gauge steel, 3 times folded for maximum rigidity, and must have EIA-310 standard hole-mounting pattern with U marking on the front and rear of each rail for ease of installation.
5	Single front and split rear doors should be min 75% hexagonal perforated. The front door of unit should be reversible so that it may open from either side. Doors shall be tool-less lift off and field reversible design and must allow minimum 135º door opening for ease during maintenance activity.
6	EIA rails two sets should be fully depth adjustable within 980mm use space area .19" Rails should accept tool less cable management accessories.
7	The Rack frame should be strong & durable, nine folded solid frame profile that can support minimum 1200 kg weight static load, and 800 kg dynamic load.
8	The frame shall come with two swivel casters, two fixed casters and levelling feet accessible from top when IT equipment is installed in the rack with base plinth of 100mm.

9	The roof of the racks should have cable entry/exit cut-out with brushes
10	Rack shall have the necessary hardware accessories (30 each M6 cage nuts and screws), Top, Bottom & Sides Air seal Kit (Side Air Seal Kit to be foam type with FR Rated)
11	Rack must be supplied with minimum 10 nos. of tool-less plastic blanking panels to avoid air re circulation. The rack must have open bottom design for clear space for cable entry from bottom.

IPDU

S. No	Technical Specifications
1	Each rack should have 2 IPDUs (Vertical) to be connected to the two different UPS sources A and B individually.
2	Each iPDU must be monitored at strip level & outlet level; must have power configuration of 32Amp, 230/420 V (3P), 22.0 KW with 3P+N+E (IP44) or 32Amp, 230V (1P) - 7. 4 KW; 10ft/3m power cord with 1P+N+E (IP44).
3	Single Phase and Three phase IPDU should have minimum 30 outlets of hybrid nature, which can be utilized as either C13 or C19 outlet. All IPDU shall have color LCD display to easily read display values. All outlets should provide high retention to avoid accidental dislodging of power cords via lockable power cords. The IPDU hybrid outlets should meet electrical compliance and should be UL & CE certified
4	The Bidder must provide the BIS certified power cables and the connectors must be UL certified. The power cords supplied must lock with the PDU outlets.
5	The three phase IPDUs should have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing.
6	The network card must meet UL2900-1 & IEC62443-4-2 security standards. The network card must be LCD touchscreen to navigate through and get the detailed information.
7	IPDU should have upgrade ready network card so that the feature of the PDU can

	be upgraded based on the changing business needs and the network card upgrade must not require any downtime. Network module must support secure boot to assure firmware authenticity.
8	Monitoring parameters – The IPDU should have monitoring and metering capability at the outlet level and Strip level and phase level. a. Voltage (V) b. Current (A) c. Power factor d. Active power (W) e. Apparent power (VA) f. Energy consumption (kwh) The PDU metering accuracy should be compliant with ANSI C12.1 and IEC 62053-21 at 1% accuracy class requirements for strip and outlet level.
9	Network communication – PDU should have minimum one Network Port 10/100/1000 Mbps and another 10/100 Mbps. IPDU should support communication protocols including DHCP, HTTP, HTTPS, Ipv4, Ipv6, LDAP, NTP, RADIUS, RSTP, SSH, SMTP, SSL, SNMP (v1, v2, v3), Syslog. Communication module should be hot-swappable, so that it can be replaced without powering off the PDU.
10	The IPDU should support the fault tolerant daisy chain minimum 32 units to reduce network port requirement and ensure continuous flow of data on network to monitoring tool/BMS/DCIM even a break in daisy chain occurs.
11	IPDU should support monitoring environmental conditions within the cabinet using additional sensors to ensure optimal operating conditions. IPDU must support temperature, humidity, door switch position, power failure sensor etc.
12	The IPDU should support the grouping of minimum 32 IPDU and IPDU sensors in the interconnected array to create the aggregated measurements like total rack power, total row power, average power, max and min power, maximum temperature, maximum humidity, minimum temperature, minimum humidity, and the average temperature in the row without use of any additional software.

13	IPDU should have the provision to discover all the similar IPDU's in the network by logging in a single IPDU to push the firmware upgrades and configuration files to all the desired IPDU's in the network without any additional software
14	The IPDU should be high temperature grade, operating temperature up to 60°C.
15	IPDU should support configuration of user defined thresholds, reports and email alerts and send it automatically to the configured users automatically on the scheduled time intervals.
16	IPDU should support strong encryption, passwords and advanced authorization options including local permissions, LDAP/S and active directory.
17	IPDU should have LED indicators for each outlet along with the outlet number to show the status of the outlets.
18	The IPDU should have approvals form RoHS, IEC, EN, CE / UL certifications.
19	Each rack should have minimum 2 set of temperature and humidity sensors in front of rack. RS-485 cable with RJ45 connector shall be provided to connect with each IPDU.
20	The IPDU and sensors should be from the same manufacturer/OEM as of IPDU for seamless integration, configuration, data collection and service.
21	IPDU should be able to integrate with any prevalent/ industry leading DCIM software. Bidder shall integrate proposed IPDU with DCIM at Bhubaneswar DC for centralized monitoring – rack/ row/ room level. Bidder has to provide end-to-end solution to connect with DCIM. The bidder to undertake the maintenance of IPDU during the contract period.

I. Threat Intelligence Feeds

S No	Mandatory features	Compliance (Yes/No)
1	Bidder shall propose threat intel feeds from three different providers that will satisfy the respective proposed common technical specifications.	
2	The Threat Intel feed should be capable of handling at least 150K bulk IOCs enrcihment capabilities on daily basis.	

3	The solution should have advanced search capability on the data set in free text format, using search parameters/modifiers and logical operators. The properties that may be part of advanced searches must include, at least: 1. Detections and names of malware/threats by multiple cybersecurity vendors 2. Properties extracted from the static analysis of said threats (e.g. authenticode signature of executables). 3. Properties extracted from dynamic analysis (e.g. writing to registry keys). 4. Telemetry relative to where a certain threat has been observed. 5. Relationship to other entities in the data set. 6. Descriptions and profiles of actors and campaigns	
4	Files/Hashes capabilities: 1. Threat Intel Platform should have native (from same OEM) sandbox capabilities. 2. File scanning/sandboxing (reputation, static, dynamic, code analysis): atleast 1000 per month 3. Private URL scanning (reputation, static, dynamic): atleast 1000 per month	
5	The Bank shall have access to Bidders/OEM portal for Threat Intelligence. It should not have restriction on number of users.	
6	The source entity/organization from which Threat Intelligence is procured shall have the following criteria: a. The team which prepares, analyses & monitors the threat feed must have at least 50 researchers b.Threat Intelligence should Collect real time and contextual intelligence over 1 million sources.	
	API capabilities	
7	All operations and data offered by the Threat Intel feeds should be accessible through a RESTful application programming interface (API), with support for any number of integrations, including ServiceNow, IBM QRadar, SOAR, TIP etc. and should not have limitations on the number of integrations in third-party security products	
8	Should support uploading a file for analysis or querying for a specific file hash, URL, domain or IP address.	
	Threat Intel capabilities	
9	The Threat Intel feeds should provide a. Risk lists of vulnerabilities with a configurable update frequency within 24 hours b. Risk lists of Malicious IP, Malicious Domain, URL and Hash with an update frequency in very short TAT. c. Contextual and actionable intelligence with evidence to facilitate bank's team to take necessary action d. Threat actor grouping along with TTP attribution	

10	The solution should have ability to search for vulnerabilities based on: Publishing date, Severity score, Exploitation state, Exploitation consequences, Availability of mitigations etc	
11	The solution should have ability to search for Threat Actors based on: Source region, Targeted industries and regions, Associated malware and tools etc	
12	The solution should have ability to search for malware families based on: Operating system, Role of malware, such as backdoor, downloader, dropper, capabilities such as stopping or deleting a service, hiding, windows, etc	
13	The solution should have ability to search for adversarial campaigns based on: Earliest and latest activity date, Global or individually focused campaign, Targeted industries and regions, Source region.	
14	The solution should have analysis and contextualization of Cyber Threat Intelligence reports. All this information must be accessible through web reports.	
15	It should also provide actionable intellegence which includes IOC list such as IPs, CVEs, Hashesh, Rules (YARA, Sigma etc), List of associated TTPs etc.	
16	Should provide score based on severity of the Indicator based on attribution to APTs, campaigns, malware type and time.	
17	Dynamic analysis capabilities: 1. Detonation in multiple sandboxes, with coverage for Windows, OS X, Linux and Android operating systems. 2. Correlation of the execution of the samples to tactics and techniques documented in the MITRE ATT&CK standard.	
18	Threat Intel feeds should collect and analyze various Web Content related to keyword provided by Bank from Open Web, RSS, Blogs, News, Deep Web, Dark Web, Dark Markets, Custom Sources, Paste Sites.	
19	Threat Intel feed should provide at minimum the following intelligence feeds in open standard formats like CyboX, OpenIOC, Yara, STIX, TAXII etc. and there should not be any vendor proprietary format. BFSI Industry Specific Intelligence Open-source intelligence (OSINT) Financial intelligence (FININT) Tech intelligence (TECHINT) Cyber intelligence (CYBINT) Deep and Darkweb	
20	Threat Intel feed should collect real time global threat intel data, dedupe, aggregate, normalize, enrich and process threat intelligence in a holistic and actionable manner	
21	In the event of any security breach or incident on WEB (clear, deep and dark), it should be analysed and converted into intelligence reports and ingested into Threat Intel portal	
22	Threat Intel feed should atleast include information related to IOCs such as Source information (IP, Domain, URL, File hashes, vulnerabilities etc.), File formats (.exe, .doc, .pdf, .xml etc.), Geo Location, File hash values, Vulnerability details.	

23	Threat Intel feed should ensure completeness and accuracy of the intelligence information and must not miss in receiving, notifying the threat intelligence information	
24	Threat Intel feeds should be capable of continuous updation in real-time as new information or context is gathered from various sources	
25	It should support analysis with real-time trends and developments, historical view of related events, reported roles involved in the events (attackers/threat actors, targets/organizations), reported TTPs (attack vectors, malware, exploits), reported indicators (IP addresses, domains, hashes, URLs etc.) and other contextual details about the events	
26	Threat Intel feeds should have collection capabilities from sources such as attack surface data, incident response investigations, adversarial activities in open source and the dark web as well as intelligence gathered from advanced hunting performed in bank's network. Threat feed should be refreshed immediately on any new threat identification or any new attack observed around globe.	
	Dashboard capabilities	
27	It should provide dashboards and visual representation of insights and findings, which can be downloaded in various formats such as PDF, CSV, Word etc.	
28	Threat Intel feed should provide executive summary to quickly understand the vulnerabilities, Threat actor advisories, IOC/Malware advisories etc. It should include following : 1. Threat level / Severity / Score based on risk rating, exploitation state, etc 2. IOC timeline. 3. Mitigation measures 4. Impacted/ targetted solutions/OEMs 5. Sources, associated threat actors and threat intel reports	
29	Threat Intel feeds should allow to send new artifacts, for example files, and start an analysis on demand.	
30	The preoposed Threat Intel feeds shoould allow the configuration of alerts and notifications e.g. detection on IoCs/observables based on a certain YARA rule configurable by the user.	
31	The solution should provide YARA rules against the file database/ malware profiles.	
32	The solution should provide generative AI / any similar functionality to generate easy-to-understand natural language queries that explains the purpose and potential risks so that security analysts can easily identify malicious behaviour.	
33	Threat Intel feed should provide context or co-references with other IOCs. (E.g. other IP addresses within the	

	CIDR (Classless Inter-Domain Routing) and their relevant information necessary to evaluate risk)	
	Other capabilities	
34	The solution should offer deep asset discovery beyond initial internet crawls and scans to discover and map unknown assets that would otherwise remain unmanaged.	
35	The solution should provide the Attack Surface Management methodology to discover assets and technology.	
36	The solution should allow exporting the information in a structured format that can be processed automatically, for example JSON, CSV or XML, STIX, TAXII etc	
37	The solution should monitor a following use cases : Advanced Persistent Threat, Anonymization, Botnet, Compromised Infrastructure, Confidential Document Leak, Credential Leak, Credit Card Leak, Exploit, Information Leak, Malicious Activity, Malicious Infrastructure, Malware, Personal Information Disclosure, Phishing, Ransomware, Ransomware Victim Listing etc	
38	The solution should analyze or reverse engineer malware. This malware analyst/reverse engineer assistant should produce natural language summaries of file capabilities without any license limitations.	
39	It should have out of box integration with Bank's SOAR and TIP platforms. Threat Intellegence feed provider (OEM) should be able to provide custom API integrations as and when required by Bank to integrate with any other solutions deployed in Bank environment.	
40	Bank has few integrated Threat Intel feeds which must be excluded for the purpose of proposing Threat intellegence feeds. which threat intel is already being received in Banks environment.	
41	Proposals for new threat intelligence feeds must clearly identify and exclude any feeds currently utilized by the Bank's security infrastructure. The proposed solution should demonstrate how it complements and enhances, rather than duplicates, our existing threat intelligence capabilities. List of OEMs having presence in Banks environment will be shared with prospective bidders.	
	Desirable Features	**Marks**
42	The solution should have their own in-house 24/7/365 CERT/CSIRT and must have in-house capabilities to engage with law enforcement agencies.	10
43	Threat Intel provider must be established more than 10 years ago (from date of issuance of this RFP) that having much of experience in threat intelligence collection	10

44	The solution should offer browser extensions to contextualize indicators contained in third-party interfaces and automatic or semi-automatic analysis of files and network indicators encountered by its users. It should provide instant correlation with Risk score, triggered risk rules and evidence that assist in prioritization for IP address, Domains, URL, Hashes or Vulnerabilities present on any web page. The risk scoring functionality should also have the capability to update the scoring of IOCs based on sightings in the bank environment.	10
45	Threat Intelligence Feed should contain data on Command-and-Control servers and DNS Exfiltrators.	10
46	There should be categorisation of Threat Intel into various categories like BFSI sector specific, India specific as well as threat actor specific, type of IOCs etc.	20
47	Proposed Solution shall allow to add IOC/IOA sources in platform such as (but not limited to) TOR Project official exit nodes, Ransomware Tracker, etc. based on (not limited to) IP Address, URL's, Domain, Files Hashes, (MD 5, SHA1, SHA256 etc..) hostnames, email, CIDR rules, File paths etc.	20
48	IT should integrate with bank's existing SOC tools, vulnerability management tools such as SIEM, Deep Analysis tools, EDR, Firewalls, UEBA, DNS Proxy and other devices to integrate the feeds.	20

Annex IV- Bill of Material (BOM) without price

Indicative Bill of Material (Hardware, Software, Services etc.) with 3 years Warranty and 2 years Support - Technical Bid										
A. Hardware requirement for Bhubaneswar Data Centres with 3 years Warranty										
S. No.	**Solution / Device**	**Category as per Annexure III – Technical Specifications**	**Quantity for DC buildings in Bhubaneswar**				**Proposed Stack by Bidder**			**Remarks**
			Payment DC	**Non-Payment DC**	**Testing and UAT DC**	**Admin Building**	**OEM**	**Item name & Model No.**	**Part Code**	
1	MZ Firewall + IPS	**A**	2	2	2	0				**Bidder shall propose different OEM for Category A - Internal Firewall and Category B - Perimeter Firewall**
2	Perimeter & DMZ Firewall + IPS + Proxy	**B**	4	4	4	2				
3	Management & Backbone Firewalls + IPS	**B**	2	2	2	0				
4	Malware Sandboxing (For Perimeter Firewall)	**C**	1	1	1	1				
5.1	Central Firewall Manager (License + Log Collectors)	**A**	1 (Primary)	1 (DR)	0	0				
5.2	Central Firewall Manager (License + Log Collectors)	**B**	1 (Primary)	1 (DR)	0	0				
6	Web Application Firewall	**D**	2	2	2	0				
7	DMZ Server Load Balancer	**E**	2	2	2	0				
8	Perimeter SSL Orchestrator	**F**	2	2	2	0				
9	Perimeter Global Server Load Balancer / Link Load Balancer	**G**	2	2	2	0				
10	Perimeter DDoS	**H**	2	2	2	0				
11	Racks and IPDU	Bidder to propose quantities based on proposed devices from S No. 1 to 10 above as per respective specifications in Annexure III .								
12	Any other passive component required									

12.1	Component 1									
12.2	Component 2									
12.3	Component 3									
12.4	Component 4									
12.5	Component 5									
B. Associated licenses for Hardware for Bhubaneswar Data Centres										
13	**Associated Licenses for MZ firewall + IPS mentioned at serial no. 1**	A								
13.1	License component 1									
13.2	License component 2									
13.3	License component 3									
13.4	License component 4									
13.5	License component 5									
14	**Associated licenses for Perimeter & DMZ Firewall + IPS + Proxy mentioned at serial no. 2**	B								
14.1	License component 1									
14.2	License component 2									
14.3	License component 3									
14.4	License component 4									
14.5	License component 5									
15	**Associated licenses for Management & Backbone Firewalls + IPS mentioned at serial no. 3**	B								
15.1	License component 1									
15.2	License component 2									
15.3	License component 3									
15.4	License component 4									
15.5	License component 5									

16	**Associated licenses for Malware Sandboxing (For perimeter Firewalls) mentioned at serial no. 4**	C								
16.1	License component 1									
16.2	License component 2									
16.3	License component 3									
16.4	License component 4									
16.5	License component 5									
17	**Associated licenses for Central Firewall Manager (License + Log Collectors) mentioned at serial no. 5.1 and 5.2**	A & B								
17.1	License component 1									
17.2	License component 2									
17.3	License component 3									
17.4	License component 4									
17.5	License component 5									
18	**Associated licenses for Web Application Firewall mentioned at serial no. 6**	D								
18.1	License component 1									
18.2	License component 2									
18.3	License component 3									
18.4	License component 4									
18.5	License component 5									
19	**Associated licenses for DMZ Server Load Balancer mentioned at serial no. 7**	E								
19.1	License component 1									
19.2	License component 2									
19.3	License component 3									

19.4	License component 4									
19.5	License component 5									
20	**Associated licenses for Perimeter SSL Orchestrator mentioned at serial no. 8**	F								
20.1	License component 1									
20.2	License component 2									
20.3	License component 3									
20.4	License component 4									
20.5	License component 5									
21	**Associated licenses for Perimeter Global Server Load Balancer / Link Load Balancer mentioned at serial no. 9**	G								
21.1	License component 1									
21.2	License component 2									
21.3	License component 3									
21.4	License component 4									
21.5	License component 5									
22	**Associated licenses for Perimeter DDoS mentioned at serial no. 10**	H								
22.1	License component 1									
22.2	License component 2									
22.3	License component 3									
22.4	License component 4									
22.5	License component 5									

AA. Passive Component (Quantities are only indicative in nature, actual quantity will be arrived post site survey)						
12.2	**Component description**	**Total Qty**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
12.2.1	**Copper Structured Cabling**					Bidder shall ensure that the DC cable design, layout and operational considerations may be TIA 942 standard compliant.
i.	High Speed Gigabit Ethernet U/UTP 250MHz Class E, LSZH Cable (UTP Cable Box), 305 Mtr	100		0	0	
ii.	Copper Panel Unshielded 48 Port Unloaded 1U wire manager included	100		0	0	
iii.	Back Box UK Style & Shuttered single phase plate	100		0	0	
iv.	Keystone Unshielded Outlet, 180DG C6, Black & White	100		0	0	
12.2.1	**Copper Patch Cords**					
i.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 3 Mtr	100		0	0	
ii.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 5 Mtr	100		0	0	
iii.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 10 Mtr	100		0	0	
12.2.3	**Fiber Structured Cabling**					
i.	High Link Fiber Optic, Tight Buffered Indoor Cable, FR LSZH, OM4, 12 Cores (in meter)	100		0	0	
ii.	Fiber Panel Sliding 2 Cutout, Adapter Plate Loaded with 12 LC duplex, Blank Adapter Plate, 24 LCU Pigtails, Splice Tray, OM4, 1U	100		0	0	
iii.	High Link Fiber Optic, Tight Buffered Indoor Cable, FR LSZH, OM4, 24 Cores (in meter)	100		0	0	
iv.	Fiber Panel Sliding 2 Cutout, Adapter Plate Loaded with 24 LC duplex, Blank Adapter Plate, 48 LCU Pigtails, Splice Tray, OM4, 1U	100		0	0	

12.2.4	**Fiber Patch Cords**					
i.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 3M	100		0	0	
ii.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 5M	100		0	0	
iii.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 10M	100		0	0	
12.2.5	**Installation & Related Services incl Certification**	1		0	0	
12.2.6	**Any Other component, if required**					
i.	Component 1			0	0	
ii.	Component 2			0	0	
iii.	Component 3			0	0	
iv.	Component 4			0	0	
v.	Component 5			0	0	
	Total Cost of Passive Component- Sub total-AA				**0**	

C. Additional Hardware requirement for existing Data Centres with 3 years Warranty									
Sl. No.	**Solution / Device**	**Category as per Annexure III – Technical Specifications**	**PDC, Kharghar**	**ODC, Belapur**	**DRDC, Nagpur**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
23	Malware Sandboxing	**C**	1	1	1				**Bidder to ensure that the proposed devices shall be compatible, implemented and integrated within the existing security architecture, design and infrastructure at PDC, ODC & DRDC**
24	Web Application Firewall	**D**	4	6	4				
25	DMZ Server Load Balancer	**E**	2	2	2				

26	Perimeter DDOS	**H**	2	2	2				
26.A	Perimeter Firewall (with required VPN licenses)	B	2	2	2				**Device should support VPN functionality.**
27	Racks and IPDU	Bidder to propose quantities based on proposed devices from S No. 23 to 26.A above and feasibility study of rack space in current DCs as per respective specifications in Annexure III							

D. Associated licenses for Hardware for Existing Data Centres as specified above										
28	**Associated licenses for Malware Sandboxing mentioned at serial no. 23**	C								
28.1	License component 1									
28.2	License component 2									
28.3	License component 3									
28.4	License component 4									
28.5	License component 5									
29	**Associated licenses for Web Application Firewall mentioned at serial no. 24**	D								
29.1	License component 1									
29.2	License component 2									
29.3	License component 3									
29.4	License component 4									
29.5	License component 5									
30	**Associated licenses for DMZ Server Load Balancer mentioned at serial no. 25**	E								
30.1	License component 1									
30.2	License component 2									
30.3	License component 3									
30.4	License component 4									

30.5	License component 5									
31	**Associated licenses for Perimeter DDoS mentioned at serial no. 26**	H								
31.1	License component 1									
31.2	License component 2									
31.3	License component 3									
31.4	License component 4									
31.5	License component 5									
31 (A)	**Associated licenses for Perimeter Firewall mentioned at serial no. 26 A**	H								
31 (A).1	License component 1									
31 (A).2	License component 2									
31(A).3	License component 3									
31 (A).4	License component 4									
31 (A).5	License component 5									

E. Implementation services: Plan, Design, Implementation, Onboarding/Migration, Audit, Validation, Certification and Review - ONE TIME					
32.1	**Plan, Design, Implementation of total solution, Services Onboarding / Migration, Audit, Validation, Certification, and review of implementation for line items mentioned in serial number 1 to 22 (For Bhubaneswar Data Centres)**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
i	Internal Firewall Solution				Bidder must provide detailed services as per
ii	Perimeter Firewall Solution				
iii	Web Application Firewall				

iv	DMZ Server Load Balancer				Scope of Implementation
v	Perimeter SSL Orchestrator				
vi	Perimeter Global Server Load Balancer / Link Load Balancer				
vii	Perimeter DDoS				
viii	Racks and IPDU				
32.2	**Implementation services by System Integrator / Bidder for line items mentioned in serial number 1 to 22 (For Bhubaneswar Data Centres)**				
32.3	**Plan, Design, Implementation of total solution, Services Onboarding / Migration, Audit, Validation, Certification and review of implementation for line items mentioned in serial number 23 to 31 (For Existing Data Centres at Kharghar, Belapur and Nagpur)**				Bidder must provide detailed services as per Scope of Implementation
i	Malware Sandboxing				
ii	Web Application Firewall				
iii	DMZ Server Load Balancer				
iv	Perimeter DDOS				
v.	Perimeter Firewall (with required VPN licenses)				
vi.	Racks and IPDU				
32.4	**Implementation services by System Integrator / Bidder for line items mentioned in serial number 23 to 31 (For existing Data Centres at Kharghar, Belapur and Nagpur)**				

F. Comprehensive AMC/ATS support for all the Hardware/Software requirement for Bhubaneswar Data Centres for Year 4										
S. No.	**Solution / Device**	**Category as per Annexure III – Technical Specifications**	**Quantity for DC buildings in Bhubaneswar**				**Proposed Stack by Bidder**			**Remarks**
			Payment DC	**Non Payment DC**	**Testing and UAT DC**	**Admin Building**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	
33.1	MZ Firewall + IPS	**A**	2	2	2	0				

33.2	Perimeter & DMZ Firewall + IPS + Proxy	**B**	4	4	4	2				**Bidder shall propose different OEM for Category A - Internal Firewall and Category B - Perimeter Firewall**
33.3	Management & Backbone Firewalls + IPS	**B**	2	2	2	0				
33.4	Malware Sandboxing (For Perimeter Firewall)	**C**	1	1	1	1				
33.5	Central Firewall Manager (License + Log Collectors)	**A**	1 (Primary)	1 (DR)	0	0				
33.6	Central Firewall Manager (License + Log Collectors)	**B**	1 (Primary)	1 (DR)	0	0				
33.7	Web Application Firewall	**D**	2	2	2	0				
33.8	DMZ Server Load Balancer	**E**	2	2	2	0				
33.9	Perimeter SSL Orchestrator	**F**	2	2	2	0				
33.10	Perimeter Global Server Load Balancer / Link Load Balancer	**G**	2	2	2	0				
33.11	Perimeter DDoS	**H**	2	2	2	0				
33.12	Racks and IPDU	Bidder to propose quantities based on proposed devices from S No. 1 to 10 above as per respective specifications in Annexure III								
33.13	Component 1									
33.14	Component 2									
33.15	Component 3									
33.16	Component 4									
33.17	Component 5									

G. Comprehensive AMC/ATS support services for all the Hardware/Software requirement for existing Data Centres for Year 4									
Sl. No.	**Solution / Device**	**Category as per Annexure III – Technical Specifications**	**PDC, Kharghar**	**ODC, Belapur**	**DRDC, Nagpur**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
34.1	Malware Sandboxing	**C**	1	1	1				**Bidder to ensure that the proposed devices shall be compatible, implemented and integrated within the existing security architecture, design and infrastructure at PDC, ODC & DRDC**
34.2	Web Application Firewall	**D**	4	6	4				
34.3	DMZ Server Load Balancer	**E**	2	2	2				
34.4	Perimeter DDOS	**H**	2	2	2				
34.5	Perimeter Firewall (with required VPN licenses)	B	2	2	2				**Device should support VPN functionality.**
34.6	Racks and IPDU	Bidder to propose quantities based on proposed devices from S No. 22 to 25 above and feasibility study of rack space in current DCs as per respective specifications in Annexure III							

H. Facility Management Services (Help Desk & Operations for Year 1 to 5) for Data Centres							
35.1	**Facility Management Services for Bhubaneswar DCs**						
	Solution	**Resources**	**No of resources required**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
i	Next Generation Firewall with IPS, Proxy, Malware Sandboxing etc. & Anti-DDOS	L1 - Bidder	13				Bidder must provide FMS resources in adherence to FMS scope of work and
		L2 - Bidder	8				
		L3 Technical Lead	2				
		OEM Resident Engineer for Internal Firewall Solution	1				

		OEM Resident Engineer for Perimeter Firewall Solution	1						qualifications in RFP
ii	WAF and SSLO	L1– Bidder	8						
		L2 – Bidder	5						
		L3 - Technical Lead	1						
		OEM Resident Engineer for WAF	1						
		OEM Resident Engineer for SSLO	1						
iii	Server Load Balancer & GSLB	L1 - Bidder	5						
		L2 - Bidder	4						
		L3 - Technical Lead	1						
		OEM Resident Engineer	1						
iv	Project Operation	Operations Manager - Bidder	1						
35.2	**Facility Management Services for Existing DCs - PDC, ODC and DRDC**								
	Solution	**Resources**	**PDC**	**ODC**	**DRDC**				Bidder must provide FMS resources in adherence to FMS scope of work and qualifications in RFP
i	WAF	L1 - Bidder	5	5	5				
		L2 - Bidder	5	5	5				
		L3 - Technical Lead	1	0	1				
		OEM Resident Engineer for WAF	1	0	1				
ii	Server Load Balancer (SLB)	L1 - Bidder	2	2	2				
		L2 - Bidder	2	2	2				
		L3 - Technical Lead	1	0	1				
iii	Anti- DDoS	L1 - Bidder	2	2	2				
		L2 - Bidder	2	2	2				
		L3 - Technical Lead	1	0	1				
iv	Perimeter Firewall	L1 - Bidder	2	2	2				

		L2 - Bidder	2	2	2				
		L3 - Technical Lead	1	0	0				

I. Other Services - Highest / Premium Support from OEM (For Year 1 onwards)										
	Highest / Premium Support from each OEM	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
36	Direct Highest / Premium Support with respective OEMs for all the security solutions procured under this RFP (on 24x7x365 basis)									Specify documentation/datasheet specifying the details of all the deliverables like service part code, features etc. for all those OEMs
i.	Internal Firewall Solution									
ii.	Perimeter Firewall Solution									
iii.	Web Application Firewall									
iv.	DMZ Server Load Balancer									
v.	Perimeter SSL Orchestrator									
vi.	Perimeter Global Server Load Balancer / Link Load Balancer									
vii	Perimeter DDoS									
37	Yearly Comprehensive onsite review by OEM for Bhubaneswar DCs									
38	Yearly Comprehensive onsite review by OEM for Existing DCs									

39	Subscription to Cyber Threat Intelligence Feed 1									**Bidder shall propose different OEM for Threat Intelligence Feed 1, 2 & 3**
40	Subscription to Cyber Threat Intelligence Feed 2									
41	Subscription to Cyber Threat Intelligence Feed 3									

"24x7" shifts of L1 and L2 shall be ensured wherever required by including the resources across all the DCs

The above BOM is just INDICATIVE. Bidders to give complete details item wise.

The Technical Bid shall contain no financial/commercial details. Proposals with Technical Bid containing prices shall be outrightly rejected.

Any decision in this regard by Bank shall be final, conclusive, and binding on the Bidder.

Any additional component required for implementing the total solution apart from above will be supplied and installed by Bidder Free of Cost at the time of going Live or during contract period.

RBI reserves the right to alter the requirements/quantities of the proposed solutions under the project.

Annex V - Submission Checklist

Submission Checklist for Technical Bid/Assessment of Eligibility

The bidder has to ensure that the following have been submitted as a part of the RFP submission process.

Failure to provide any of the documents as detailed below could lead to the disqualification of the bidder from the bid.

The following documents/items need to be submitted:

Items	Submitted (Bidder)	Verified (RBI)
Compliance to Technical Specifications	☐	☐
Technical Bid Form (Bill of Material without prices)	☐	☐
Self-evaluation of Technical Evaluation sheet	☐	☐
Deviation from Technical Specification	☐	☐
Bidder's Application Form	☐	☐
Undertaking from Bidder on Support	☐	☐
Undertaking from Bidder on Products	☐	☐
Letter of Authority	☐	☐
Earnest Money Deposit	☐	☐
Bidders Profile Form	☐	☐
Integrity Pact	☐	☐
Non-Disclosure Agreement	☐	☐
Self-Declaration Sexual Harassment of Women at	☐	☐
Maintenance and Service Support of the Bidder	☐	☐
Undertaking from OEM on Support	☐	☐
Bidder eligibility criteria (Necessary documents in support of this)	☐	☐
Manufacturer Authorization Format	☐	☐
Product Brochures containing detailed description of essential technical and performance characteristics of all offered components	☐	☐

Purchase Order/ Reference Letter with letter of satisfaction from client in support of Experience claimed (Each Component with size, level and duration of engagement)	□	□
Signed copy of all other Annexures part of RFP except commercial BID	□	□
Documentary evidence for “Stage of product Life Cycle” □ from the information/documents available in public domain.	□	□
Undertaking for back-to-back commitment from the OEM	□	□

Submission Checklist for Commercial Bid

The following documents need to be provided by the Bidder for the Commercial Bid in a separately sealed cover.

Commercial Bid Documents	Submitted (Bidder)	Verified (Bank)
Commercial Bid	□	□
Compliance Certificate for Commercial Bid	□	□

Annex VI - Commercial Bid Form

Indicative Bill of Material (Hardware, Software, Services etc.) with 3 years Warranty and 2 years Support - Commercial Bid											
A. Hardware requirement for Bhubaneswar Data Centres with 3 years Warranty											
S. No.	Solution / Device	Category as per Annexure III B – Technical Specifications	Quantity for DC buildings in Bhubaneswar				Total Qty	Unit Price	Taxes	Total Price with taxes	Remarks
			Payment DC	Non-Payment DC	Testing and UAT DC	Admin Building					
1	MZ Firewall + IPS	**A**	2	2	2	0	6		0	0	**Bidder shall propose different OEM for Category A - Internal Firewall and Category B - Perimeter Firewall**
2	Perimeter & DMZ Firewall + IPS + Proxy	**B**	4	4	4	2	14		0	0	
3	Management & Backbone Firewalls + IPS	**B**	2	2	2	0	6		0	0	
4	Malware Sandboxing (For Perimeter Firewall)	**C**	1	1	1	1	4		0	0	
5.1	Central Firewall Manager (License + Log Collectors)	**A**	1 (Primary)	1 (DR)	0	0	0		0	0	
5.2	Central Firewall Manager (License + Log Collectors)	**B**	1 (Primary)	1 (DR)	0	0	0		0	0	
6	Web Application Firewall	**D**	2	2	2	0	6		0	0	
7	DMZ Server Load Balancer	**E**	2	2	2	0	6		0	0	
8	Perimeter SSL Orchestrator	**F**	2	2	2	0	6		0	0	
9	Perimeter Global Server Load Balancer / Link Load Balancer	**G**	2	2	2	0	6		0	0	
10	Perimeter DDoS	**H**	2	2	2	0	6		0	0	
11	Racks and IPDU						0		0	0	Bidder to propose quantities based on proposed devices from S No. 1 to 10 above as per respective specifications in Annexure IIIB.
12	**Any other passive component required**										
12.1	Component 1						0		0	0	
12.2	Component 2						0		0	0	
12.3	Component 3						0		0	0	
12.4	Component 4						0		0	0	
12.5	Component 5						0		0	0	
Sub Total A										**0**	

B. Associated licenses for Hardware for Bhubaneswar Data Centres											
S. No.	Solution / Device	Category as per Annexure III B – Technical Specifications	Quantity for DC buildings in Bhubaneswar				Total Qty	Unit Price	Taxes	Total Price with taxes	Remarks
			Payment DC	Non-Payment DC	Testing and UAT DC	Admin Building					
13	**Associated Licenses for MZ firewall + IPS mentioned at serial no. 1**	A									
13.1	License component 1						0		0	0	
13.2	License component 2						0		0	0	
13.3	License component 3						0		0	0	
13.4	License component 4						0		0	0	
13.5	License component 5						0		0	0	
14	**Associated licenses for Perimeter & DMZ Firewall + IPS + Proxy mentioned at serial no. 2**	B									
14.1	License component 1						0		0	0	
14.2	License component 2						0		0	0	
14.3	License component 3						0		0	0	
14.4	License component 4						0		0	0	
14.5	License component 5						0		0	0	
15	**Associated licenses for Management & Backbone Firewalls + IPS mentioned at serial no. 3**	B									
15.1	License component 1						0		0	0	
15.2	License component 2						0		0	0	
15.3	License component 3						0		0	0	
15.4	License component 4						0		0	0	
15.5	License component 5						0		0	0	
16	**Associated licenses for Malware Sandboxing (For perimeter Firewalls) mentioned at serial no. 4**	C									
16.1	License component 1						0		0	0	
16.2	License component 2						0		0	0	
16.3	License component 3						0		0	0	
16.4	License component 4						0		0	0	
16.5	License component 5						0		0	0	
17	**Associated licenses for Central Firewall Manager (License + Log Collectors) mentioned at serial no. 5.1 and 5.2**	A & B									
17.1	License component 1						0		0	0	
17.2	License component 2						0		0	0	
17.3	License component 3						0		0	0	
17.4	License component 4						0		0	0	
17.5	License component 5						0		0	0	
18	**Associated licenses for Web Application Firewall mentioned at serial no. 6**	D									
18.1	License component 1						0		0	0	
18.2	License component 2						0		0	0	
18.3	License component 3						0		0	0	
18.4	License component 4						0		0	0	
18.5	License component 5						0		0	0	
19	**Associated licenses for DMZ Server Load Balancer mentioned at serial no. 7**	E									
19.1	License component 1						0		0	0	
19.2	License component 2						0		0	0	
19.3	License component 3						0		0	0	
19.4	License component 4						0		0	0	
19.5	License component 5						0		0	0	
20	**Associated licenses for Perimeter SSL Orchestrator mentioned at serial no. 8**	F									
20.1	License component 1						0		0	0	
20.2	License component 2						0		0	0	
20.3	License component 3						0		0	0	
20.4	License component 4						0		0	0	
20.5	License component 5						0		0	0	
21	**Associated licenses for Perimeter Global Server Load Balancer / Link Load Balancer mentioned at serial no. 9**	G									
21.1	License component 1						0		0	0	
21.2	License component 2						0		0	0	
21.3	License component 3						0		0	0	
21.4	License component 4						0		0	0	
21.5	License component 5						0		0	0	
22	**Associated licenses for Perimeter DDoS mentioned at serial no. 10**	H									
22.1	License component 1						0		0	0	
22.2	License component 2						0		0	0	
22.3	License component 3						0		0	0	
22.4	License component 4						0		0	0	
22.5	License component 5						0		0	0	
Sub Total B										**0**	
I.Total cost of Hardware and Software for Bhubaneswar Data Centres										**0**	

AA. Passive Component (Quantities are only indicative in nature, actual quantity will be arrived post site survey)						
12.2	**Component description**	**Total Qty**	**Proposed OEM**	**Item name & Model No.**	**Part Code**	**Remarks**
12.2.1	**Copper Structured Cabling**					Bidder shall ensure that the DC cable design, layout and operational considerations may be TIA 942 standard compliant.
i.	High Speed Gigabit Ethernet U/UTP 250MHz Class E, LSZH Cable (UTP Cable Box), 305 Mtr	100		0	0	
ii.	Copper Panel Unshielded 48 Port Unloaded 1U wire manager included	100		0	0	
iii.	Back Box UK Style & Shuttered single phase plate	100		0	0	
iv.	Keystone Unshielded Outlet, 180DG C6, Black & White	100		0	0	
12.2.1	**Copper Patch Cords**					
i.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 3 Mtr	100		0	0	
ii.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 5 Mtr	100		0	0	
iii.	High Speed Gigabit 28AWG U/UTP Patch Cored Gray, LSZH, 6C, 10 Mtr	100		0	0	
12.2.3	**Fiber Structured Cabling**					
i.	High Link Fiber Optic, Tight Buffered Indoor Cable, FR LSZH, OM4, 12 Cores (in meter)	100		0	0	
ii.	Fiber Panel Sliding 2 Cutout, Adapter Plate Loaded with 12 LC duplex, Blank Adapter Plate, 24 LCU Pigtails, Splice Tray, OM4, 1U	100		0	0	
iii.	High Link Fiber Optic, Tight Buffered Indoor Cable, FR	100		0	0	
iv.	Fiber Panel Sliding 2 Cutout, Adapter Plate Loaded with 24 LC duplex, Blank Adapter Plate, 48 LCU Pigtails, Splice Tray, OM4, 1U	100		0	0	
12.2.4	**Fiber Patch Cords**					
i.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 3M	100		0	0	
ii.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 5M	100		0	0	
iii.	High Link LCU to LCU Fiber Optic Patch Cord, Duplex, OM4, 10M	100		0	0	
12.2.5	**Installation & Related Services incl Certification**	1		0	0	
12.2.6	**Any Other component, if required**					
i.	Compoent 1			0	0	
ii.	Compoent 2			0	0	
iii.	Compoent 3			0	0	
iv.	Compoent 4			0	0	
v.	Compoent 5			0	0	
	Total Cost of Passive Component- Sub total-AA				**0**	

C. Additional Hardware requirement for existing Data Centres with 3 years Warranty and 2 years Support										
S. No.	**Solution / Device**	**Category as per Annexure III B – Technical Specifications**	**PDC, Kharghar**	**ODC, Belapur**	**DRDC, Nagpur**	**Total Qty**	**Unit Price**	**Taxes**	**Total Price with taxes**	**Remarks**
23	Malware Sandboxing	**C**	1	1	1	3		0	0	Bidder to ensure that the proposed devices shall be compatible, implemented and integrated within the existing security architecture, design and infrastructure at PDC, ODC & DRDC
24	Web Application Firewall	**D**	4	6	4	14		0	0	
25	DMZ Server Load Balancer	**E**	2	2	2	6		0	0	
26	Perimeter DDOS	**H**	2	2	2	6		0	0	
26A	Perimeter Firewall	**B**	2	2	2	6		0	0	Device should support VPN functionality
27	Racks and IPDU					0		0	0	Bidder to propose quantities based on proposed devices from S No. 23 to 26A above and feasibility study of rack space in current DCs as per respective specifications in Annexure IIIB
	Sub Total A								**0**	

D. Associated licenses for Hardware for Existing Data Centres										
S. No.	**Solution / Device**	**Category as per Annexure III B – Technical Specifications**	**PDC, Kharghar**	**ODC, Belapur**	**DRDC, Nagpur**	**Total Qty**	**Unit Price**	**Taxes**	**Total Price with taxes**	**Remarks**
28	**Associated licenses for Malware Sandboxing mentioned at serial no. 23**	C								
28.1	License component 1					0		0	0	
28.2	License component 2					0		0	0	
28.3	License component 3					0		0	0	
28.4	License component 4					0		0	0	
28.5	License component 5					0		0	0	
29	**Associated licenses for Web Application Firewall mentioned at serial no. 24**	D								
29.1	License component 1					0		0	0	
29.2	License component 2					0		0	0	
29.3	License component 3					0		0	0	
29.4	License component 4					0		0	0	
29.5	License component 5					0		0	0	
30	**Associated licenses for DMZ Server Load Balancer mentioned at serial no. 25**	E								
30.1	License component 1					0		0	0	
30.2	License component 2					0		0	0	
30.3	License component 3					0		0	0	
30.4	License component 4					0		0	0	
30.5	License component 5					0		0	0	
31	**Associated licenses for Perimeter DDoS mentioned at serial no. 26**	H								
31.1	License component 1					0		0	0	
31.2	License component 2					0		0	0	
31.3	License component 3					0		0	0	
31.4	License component 4					0		0	0	
31.5	License component 5					0		0	0	
31 (A)	**Associated licenses for Perimeter Firewall mentioned at serial no. 26A**	H								
31(A).1	License component 1					0		0	0	
31(A).2	License component 2					0		0	0	
31 (A).3	License component 3					0		0	0	
31 (A).4	License component 4					0		0	0	
31 (A).5	License component 5					0		0	0	
	Sub Total B								**0**	

II.Total cost of Hardware and Software for existing DCs	**0**	

E. Implementation services: Plan, Design, Implementation, Onboarding/Migration, Audit, Validation, Certification and Review - ONE TIME					
32.1	**Plan, Design, Implementation of total solution, Services Onboarding / Migration, Audit, Validation, Certification, and review of implementation for line items mentioned in serial number 1 to 22 (For Bhubaneswar Data Centres)**	**Unit Price**	**Taxes**	**Total Price with taxes**	**Remarks**
i	Internal Firewall Solution		0	0	
ii	Perimeter Firewall Solution		0	0	
iii	Web Application Firewall		0	0	
iv	DMZ Server Load Balancer		0	0	
v	Perimeter SSL Orchestrator		0	0	
vi	Perimeter Global Server Load Balancer / Link Load Balancer		0	0	Bidder must provide detailed services as per Scope of Implementation
vii	Perimeter DDoS		0	0	
viii	Racks and IPDU		0	0	
32.2	**Implementation services by System Integrator / Bidder for line items mentioned in serial number 1 to 22 (For Bhubaneswar Data Centres)**		0	0	
Sub Total A			**0**	**0**	
32.3	**Plan, Design, Implementation of total solution, Services Onboarding / Migration, Audit, Validation, Certification and review of implementation for line items mentioned in serial number 23 to 31A (For Existing Data Centres at Kharghar, Belapur and Nagpur)**	**Unit Price**	**Taxes**	**Total Price with taxes**	
i	Malware Sandboxing		0	0	
ii	Web Application Firewall		0	0	Bidder must provide detailed services as per Scope of Implementation
iii	DMZ Server Load Balancer		0	0	
iv	Perimeter DDOS		0	0	
v	Perimeter Firewall (with required VPN licenses)		0	0	
vi	Racks and IPDU		0	0	
32.4	**Implementation services by System Integrator / Bidder for line items mentioned in serial number 23 to 31A (For existing Data Centres at Kharghar, Belapur and Nagpur)**		0	0	
Sub Total B			**0**	**0**	
III. Implementation Cost				0	

F. Comprehensive AMC/ATS support for all the Hardware/Software requirement for Bhubaneswar Data Centres for Year 4											
S. No.	Solution / Device	Category as per Annexure III B – Technical Specifications	Quantity for DC buildings in Bhubaneswar				Total Qty	Unit Price	Taxes	Total Price with taxes	Remarks
			Payment DC	Non-Payment DC	Testing and UAT DC	Admin Building					
33.10	MZ Firewall + IPS	A	2	2	2	0	6		0	0	Bidder shall propose different OEM for Category A - Internal Firewall and Category B - External Firewall
33.20	Perimeter & DMZ Firewall + IPS + Proxy	B	4	4	4	2	14		0	0	
33.30	Management & Backbone Firewalls + IPS	B	2	2	2	0	6		0	0	
33.40	Malware Sandboxing (For Perimeter Firewall)	C	1	1	1	1	4		0	0	
33.50	Central Firewall Manager (License + Log Collectors)	A	1 (Primary)	1 (DR)	0	0	0		0	0	
33.60	Central Firewall Manager (License + Log Collectors)	B	1 (Primary)	1 (DR)	0	0	0		0	0	
33.70	Web Application Firewall	D	2	2	2	0	6		0	0	
33.80	DMZ Server Load Balancer	E	2	2	2	0	6		0	0	
33.90	Perimeter SSL Orchestrator	F	2	2	2	0	6		0	0	
33.10	Perimeter Global Server Load Balancer / Link Load Balancer	G	2	2	2	0	6		0	0	
33.11	Perimeter DDoS	H	2	2	2	0	6		0	0	
33.12	Racks and IPDU						0		0	0	Bidder to propose quantities based on proposed devices from S No. 1 to 10 above as per respective specifications in Annexure IIIB
33.13	Component 1						0		0	0	
33.14	Component 2						0		0	0	
33.15	Component 3						0		0	0	
33.16	Component 4						0		0	0	
33.17	Component 5						0		0	0	

G. Comprehensive AMC/ATS support services for all the Hardware/Software requirement for existing Data Centres for Year 4										
S. No.	Solution / Device	Category as per Annexure III B – Technical Specifications	PDC, Kharghar	ODC, Belapur	DRDC, Nagpur	Total Qty	Unit Price	Taxes	Total Price with taxes	Remarks
34.1	Malware Sandboxing	C	1	1	1	3		0	0	Bidder to ensure that the proposed devices shall be compatible, implemented and integrated within the existing security architecture, design and infrastructure at PDC, ODC & DRDC
34.2	Web Application Firewall	D	4	6	4	14		0	0	
34.3	DMZ Server Load Balancer	E	2	2	2	6		0	0	
34.4	Perimeter DDOS	H	2	2	2	6		0	0	
34.5	Perimeter Firewall (with required VPN licenses)	B	2	2	2	6		0	0	Device should support VPN functionality
34.6	Racks and IPDU					0		0	0	Bidder to propose quantities based on proposed devices from S No. 22 to 25 above and feasibility study of rack space in current DCs as per respective specifications in Annexure IIIB

IV. Total AMC/ATS Cost for Year 4	0

Comprehensive Cost for AMC	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Indexed value @5% for 4th year onwards				₹ 0.00	₹ 0.00	₹ 0.00

H. Facility Management Services (Help Desk & Operations for Year 1 for Data Centres							
35.1 Facility Management Services for Bhubaneswar DCs for Year 1							
S. No.	Solution	Resources	No of resources required	Unit Price	Taxes	Total Price with taxes	Remarks
i	Next Generation Firewall with IPS, Proxy, Malware Sandboxing etc. & Anti-DDOS	L1 - Bidder	13		0	0	Bidder must provide FMS resources in adherence to FMS scope of work and qualifications in RFP. "24x7" shifts of L1 and L2 shall be ensured wherever required by including the resources across all the DCs
		L2 - Bidder	8		0	0	
		L3- Technical Lead	2		0	0	
		OEM Resident Engineer for Internal Firewall Solution	1		0	0	
		OEM Resident Engineer for External/Perimeter Firewall Solution	1		0	0	
ii	WAF and SSLO	L1 – Bidder	8		0	0	
		L2 – Bidder	5		0	0	
		L3 Technical Lead	1		0	0	
		OEM Resident Engineer for WAF	1		0	0	
		OEM Resident Engineer for SSLO	1		0	0	
iii	Server Load Balancer & GSLB	L1 - Bidder	5		0	0	
		L2 - Bidder	4		0	0	
		L3- Technical Lead	1		0	0	
		OEM Resident Engineer	1		0	0	
iv	Project Operation	Operations Manager (8x5) - Bidder	1		0	0	
	Sub Total A		53			0	

35.2 Facility Management Services for Existing DCs - PDC, ODC and DRDC for Year 1										
S. No.	Solution	Resources	PDC	ODC	DRDC	Total Qty	Unit Price	Taxes	Total Price with taxes	Bidder must provide FMS resources in adherence to FMS scope of work and qualifications in RFP. "24x7" shifts of L1 and L2 shall be ensured wherever required by including the resources across all the DCs
i	WAF	L1 - Bidder	5	5	5	15		0	0	
		L2 - Bidder	5	5	5	15		0	0	
		L3- Technical Lead	1	0	1	2		0	0	
		OEM- Resident Engineer	1	0	1	2		0	0	
ii	Server Load Balancer (SLB)	L1 - Bidder	2	2	2	6		0	0	
		L2 - Bidder	2	2	2	6		0	0	
		L3- Technical Lead	1	0	1	2		0	0	
iii	Anti- DDoS	L1 - Bidder	2	2	2	6		0	0	
		L2 - Bidder	2	2	2	6		0	0	
		L3- Technical Lead	1	0	1	2		0	0	
iv	Perimeter Firewall	L1 - Bidder	2	2	2	6		0	0	
		L2 - Bidder	2	2	2	6		0	0	
		L3- Technical Lead	1	0	0	1		0	0	
	Sub Total B		27	22	26	75			0	

I. Other Services - Highest / Premium Support from OEM (For Year 1 onwards)					
S. No	Highest / Premium Support from each OEM	Price for Year 1	Taxes	Total Price with taxes	Remarks
36	Direct Highest / Premium Support with respective OEMs for all the security solutions procured under this RFP (on 24x7x365 basis)				Specify documentation/datasheet specifying the details of all the deliverables like service part code, features etc. for all those OEMs
i.	Internal Firewall Solution		0	0	
ii.	Perimeter Firewall Solution		0	0	
iii.	Web Application Firewall		0	0	
iv.	DMZ Server Load Balancer		0	0	
v.	Perimeter SSL Orchestrator		0	0	
vi.	Perimeter Global Server Load Balancer / Link Load Balancer		0	0	
vii	Perimeter DDoS		0	0	
37	Yearly Comprehensive onsite review by OEM for Bhubaneswar DCs		0	0	
38	Yearly Comprehensive onsite review by OEM for Existing DCs		0	0	
39	Subscription to Cyber Threat Intelligence Feed 1		0	0	
40	Subscription to Cyber Threat Intelligence Feed 2		0	0	
41	Subscription to Cyber Threat Intelligence Feed 3		0	0	
	Sub Total C	0	0	0	

V. Total Services Cost for Year 1	0

Comprehensive Cost for FMS/Other Services	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Indexed value @5% for 2nd year onwards	₹ 0.00	₹ 0.00	₹ 0.00	₹ 0.00	₹ 0.00	₹ 0.00

Terms and Conditions:

I. All the Commercial values shall be quoted in Indian Rupees.

II. All the items mentioned in the technical BoM should be provided in commercial BoM.

III. The price shall be inclusive of all taxes. The tax calculation should be shown separately.

IV. Above rates shall be valid for a period of minimum one year from the date of issue of PO for any additional requirement of items quoted in BoM. After year

1, rates for procurement of additional items during the contract period will be derived based on the indexation formula as mentioned in the RFP.

V. The above-mentioned quantity of hardware, software, licenses, services and resources are indicative only and for the purpose of calculation of Total Cost of Ownership (TCO) for selection of successful bidder. The Bank reserves the right to increase or decrease the quantity based on the requirement of the Bank at the time of placement of order.

VI. Bidder shall provide quote for 1st year Facility Management cost. For TCO calculation, cost of the resources for Year 2 to 5 will be calculated with 5% escalation.

VII. Bidder shall provide quotes for 4th year AMC / ATS/ Services cost only as mentioned above. The total cost of Comprehensive AMC/ATS for Hardware and Software should be minimum 8% of the total cost of Hardware and Software. For TCO calculation, AMC cost for Year 5 will be calculated with 5% escalation.

VIII. The Bidder shall quote for Facility Management Services based on following floor limits set for each type of resource deployed for the purpose:

Type of Resource	L1	L2	L3
Floor Limit per Resource per year	10 lakhs INR	14 lakhs INR	18 lakhs INR

Place:
Date:

Signature of Authorized signatory with Seal

Annex VII - Deviations

Deviations from Technical Specifications and Terms and Conditions of the RFP

(On the letterhead of Bidder)

S No	RFP Clause and Page No. of RFP	Technical Specifications or Terms and Conditions in Tender Document	Deviation offered	Reasons and whether deviation add to any Operational efficiency in case of the systems
1				
2				
3				

Place:

Date:

Signature of Authorized signatory with seal

Note:

i. Above information in detail should be furnished in case of each component offered separately.
ii. In case of deviations from any of the terms and conditions of the tender document, it should be specified.
iii. If any deviations from the technical specifications are warranted, reasons for such variations should be specified and
iv. Whether such variations add to improvement of the overall performance of the systems, if any, should be specifically mentioned and supported by relevant technical documentation as required above

Annex VIII - Compliance Statement

(On letterhead of the Bidder)

The Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

COMPLIANCE STATEMENT

Dear Sir,

For Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

Having examined the Bid Documents including Annexes, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply, deliver, install, test, integrate, and commission all the software and hardware from <OEM Name/s> in conformity with the said Bid Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Bid.

1 We undertake, if our Bid is accepted, to comply with the delivery schedule as mentioned in the Bid Document.

We attach hereto the Bid Response as required by the Bid document, which constitutes my/our bid.

We undertake, if our Bid is accepted, to adhere to the implementation plan put forward in our Bid Response or such adjusted plan as may subsequently be mutually agreed between us and the Reserve Bank of India or its appointed representatives.

2 If our Bid Response is accepted, we will obtain a Performance Bank Guarantee in the format given in the Bid Document issued by a scheduled commercial bank in India for a sum equivalent to 10% of the contract sum for the due performance of the contract.

3 We agree to abide by this Bid and the rates quoted therein for the orders awarded by the Bank from the last day of bid submission up to the period prescribed in the Bid which shall remain binding upon us.

4 We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addenda, other documents and if required including the changes made to the original bid documents issued by RBI, provided that only the list of deviations furnished by us in the relevant Annex, which are expressly accepted by RBI and communicated to us in writing, shall form a valid and binding part of the aforesaid RFP document. RBI is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and RBI's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

5 We hereby agree to comply with all the guidelines of CVC, Government, as applicable.

6 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.

7 We agree that we are not bound to accept the lowest or any Bid Response we may receive. We also agree that you reserve the right in absolute sense to reject all or any of the goods /products specified in the Bid Response without assigning any reason whatsoever.

8 It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company /firm/organization and empowered to sign this document as well as such other documents which may be required in this connection.

9 We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in

force in India namely “Prevention of Corruption Act 1988” as amended from time to time.

6 We certify that we have provided all the information requested by RBI in the format requested for. We also understand that RBI has the exclusive right to reject this offer in case RBI is of the opinion that the required information is not provided or is provided in a different format.

Dated this ……. Day of ……2025

…….. ……

(Signature) (In the capacity of)

Duly authorized to sign the Bid Response for and on behalf of:

……

……

……

……

(Name and address of Bidding Company)

Seal/Stamp of Bidder

Annex IX- Manufacturer's Authorization Form (MAF)

(On OEM's letter head)

Manufacturer's Authorization Form

No. _____ Date: _____

Chief General Manager-in-Charge
Reserve Bank of India,
Department of Information Technology,
14th Floor, Central Office Building,
Shahid Bhagat Singh Marg,
Fort, Mumbai – 400 001

For Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

Sub: Manufacturer Authorization for your procurement needs

Dear Sir/ Madam:

We wish to take the opportunity to inform you that as a policy, <Name of OEM> business associates/Partners/System Integrator in each country carry out all the commercial transactions for <OEM products> with the customers directly and enter into contracts independent of OEM. OEM is the sole manufacturer of products like ----------, etc. which can be procured through <Name of OEM> business associates/Partners/System Integrator.

We confirm that the business associates/Partners/System Integrator (Name ……) having its registered office at (Address ……) is one such "business associates/Authorised Partners/System Integrator" for <OEM> products in India business associates/Partners/System Integrator Name …….. , among others, possesses the requisite expertise and resources to supply, renew, upgrade, install and maintain<OEM> products to you.

The “business associates/Authorised Partners/System Integrator” has been a partner with us (please mention the level of partnership) ..... Continually for the last ..... years in India and has back-to-back support available from <OEM> to meet the SLA requirement.

We also certify that the purchaser may inspect our facilities to ascertain the claims made in regard to, if necessary, to establish to its satisfaction about the OEM’s capabilities regarding their solution.

Trust that the above points suffice your requirements. Should you need any further information or clarification in this regard, please feel free to contact us.

Thanking You,

For <OEM>Authorised signatory

Name:

Designation:

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it.

Annex X - Undertaking from Bidder on Support

Undertaking from Bidder on Support
(To be furnished by the Bidders on their Letter Head)

Place:
Date:

The Chief General Manager-in-Charge,
Reserve Bank of India,
Department of Information Technology,
Central Office Building,
Shahid Bhagat Singh Marg,
Mumbai - 400 001.

Dear Sir,

Sub: Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India -

In compliance with the requirement of the tender document, we hereby undertake to give support for Hardware and Software components and maintain the 'Proposed Solution' for 5 years from the date of audit, validation and certification from the respective OEM/s. If we are unable to provide support for the above said period, then we shall upgrade the component/ sub-component with an alternative that is acceptable to the Bank at no additional cost to the Bank and without causing any performance degradation and/or project delays.

Yours faithfully,

(Signature of Authorized Signatory)
<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF
<NAME OF THE APPLICANT ORGANISATION>

Annex XI - Undertaking from OEM/s on Support

Undertaking from OEM/s on Support
(To be furnished by the OEM/s on its Letter head)

Place:
Date:

The Chief General Manager-in-Charge,
Department of Information Technology,
Central Office Building,
Shahid Bhagat Singh Marg,
Mumbai - 400 001.

Dear Sir,

Sub: Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

In compliance with the requirement of the tender document, we hereby undertake to give support for Hardware and Software components for maintenance of the 'Proposed Solution' for 5 years from the date of audit, validation and certification from the respective OEM/s. If we are unable to provide support for the above said period, then we shall upgrade the component/ sub-component with an alternative that is acceptable to the Bank at no additional cost to the Bank and without causing any performance degradation and/or project delays. We hereby undertake to comply with all Terms and Conditions of the RFP during the course of bidding and contract period.

Yours faithfully,

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Annex XII- Undertaking from Bidder on Products

Undertaking from Bidder on Products
(To be furnished by the Bidders on their Letter Head)

Place:
Date:

The Chief General Manager-in-Charge,
Reserve Bank of India,
Department of Information Technology,
Central Office,
Central Office Building,
Shahid Bhagat Singh Marg,
Mumbai - 400 001.

Dear Sir,

Sub: Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

This bears reference to our quotation Ref. ……dated…….

2. We warrant that everything to be supplied by us shall be brand new, free from all defects and faults in material, workmanship and manufacture and shall be of the highest grade and quality and consistent with the established standards for materials specification, drawings or samples if any, and shall operate properly. The application/ software is free from embedded malicious / fraudulent code. The Software and engineering support for all the equipment/devices offered in the Total Solution is available till the end of Contract Period.

We shall be fully responsible for its efficient operation.

Yours faithfully,

(Signature of Authorized Signatory)
<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Bidders Queries Proforma- Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

Contact Details		
Name of Organization submitting request (Enter Full Legal Entity name)	:	
Full formal address of the organization	:	
Tel	:	
Email	:	
Name & position of person submitting request		
Name	:	
Position	:	

S. No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description

Place:

Date:

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Annex XIV - Bidders' Profile

Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

(On Bidder's letter head)

Bidders' Profile

BIDDER DETAILS		
1	Registered name of the bidding company	
2	Established Since	
3	Address of the Registered Office	
4	Names of Directors	1. Name (with Phone Nos) 2. 3.
5	Structure chart of the organization	
6	Total Current Employees for the last 3 years	
7	Number of offices/branches in India with locations	
8	Staff Details	No of Technical staff skilled in
		No of staff for above Project Management
		Number of years of experience in providing similar solutions as per the current requirement of the Bank
9	Reference Site(s)	
10	Experience in Similar Projects: (Give details about the following with respect to the methodology followed by you in projects of similar nature in last 5 years (For each component)	
11	a) Project Name: b) Nature of Project:	
12	Project Location:	
13	Client Name:	

14	Client address:		
15	Client contact/reference person(s):	Name	
		Address – if different from above	
		Telephone	
		Mobile Phone	
		Email address	
16	Project Start date and elapsed duration		
17	Role of the Bidder (whether complete end to-end involvement or for a particular module. Any other information of relevance)		
18	Project Information: a) Hardware Installed (make/model) b) Software Product (specification) c)Disaster Recovery mechanism d) Network Topology e) Security Features f) Support/Maintenance Obligations g) Overall Architecture Implemented		
19	Escalation Matrix		
20	<<Any other information of relevance and interest to the Bank may be furnished>>		

Place:
Date:
(Signature of Authorized Signatory)
<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF
<NAME OF THE APPLICANT ORGANISATION>

Annex XV - Integrity Pact

INTEGRITY PACT

(On INR 100 stamp paper)

General

This Agreement (hereinafter called the Integrity Pact) is made on this …… Day of …….Month, 20…., between, Reserve Bank of India, established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934 having its Head Office at Mumbai 400001 (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s…….represented by Mr. / Mrs. ……, Chief Executive Officer / Authorized Representative (hereinafter called the "BIDDER / Seller" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to purchase services and goods for “Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India and the BIDDER is willing to offer / has offered the said services. The BUYER needs to adhere with all relevant laws of land, rules, regulations, economic use of resources and of fairness in its relations with the Bidder. In order to achieve these goals, the Buyer may appoint an Independent External Monitor (IEM), who will monitor the bidding process and the execution of the contract for compliance with the principles mentioned above. Shri Nageshwar Rao Koripalli, IRS (Retd.) and Shri Pramod Shripad Phalnikar, IPS (Retd.) have been appointed as an Independent External Monitors (IEMs) in RBI, either of them may act as IEM for this RFP process.

WHEREAS the BIDDER is a Private Company / Partnership / LLP / LLC, constituted in accordance with the relevant law in the matter and the BUYER is the Central Bank of the country performing its functions on behalf of the President of India.

NOW,

THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and

free from any influence / prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

Enabling the BUYER to obtain the desired said services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

1. Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favor or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will treat all BIDDERs alike and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERS.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

1.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings

under the contract would not be stalled.

2. Commitments of the Independent External Monitor (IEM)

2.1 The Buyer may appoint a competent and credible Independent External Monitor for this Pact. Shri Nageshwar Rao Koripalli, IRS (Retd.) and Shri Pramod Shripad Phalnikar, IPS (Retd.) has been appointed as an Independent External Monitor (IEM) in RBI, either of them may act as IEM for this RFP process. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

- The Bidder's accept that the Monitor has the right to access without restriction to all project documentation of the Buyer including that provided by the Bidder. The Bidder will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Sub-bidder's (if any). The Monitor is under contractual obligation to treat the information and documents of the Bidder's / Sub-bidder's with confidentiality.
- The Buyer will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have impact on the contractual relations between the Buyer and the Bidder. The parties offer to the monitor the option to participate in such meetings.
- As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Buyer and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
- The Monitor will submit a written report to the CGM (DEPARTMENT OF INFORMATION TECHNOLOGY) within 8 to 10 weeks from the date of reference or intimation to him by the Buyer and, should the occasion arise, submit proposals for correcting problematic situations.
- If the Monitor has reported to the CGM (DEPARTMENT OF

INFORMATION TECHNOLOGY), a substantiated suspicion of an offence under relevant IPC/PC Act, and the CGM (DEPARTMENT OF INFORMATION TECHNOLOGY) has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

- The word 'Monitor' would include both singular and plural.

3. Commitments of BIDDERs

3.1 The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:

- The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

- The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor , any material or immaterial benefit or other advantage , commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favor or disfavor to any person in relation to the contract or any other contract with the Government.

- BIDDERS shall disclose the name and address of Agents and Representatives and Indian BIDDERs shall disclose their foreign Principals or Associates.

- BIDDERs shall disclose the payments to be made by them to Agents/ Brokers or any other intermediary, in connection with this bid / contract.

- The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer / service provider / system integrator and has not engaged any individual or firm or company whether Indian or Foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

- The BIDDER, either while presenting the bid or during negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, Agents, Brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

- The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

- The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

- The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

- The BIDDER commits to refrain from giving any complaint directly or

through any other manner without supporting it with full and verifiable facts.

- The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

- If the BIDDER or any employee of the BIDDER or any person acting on behalf of the
- BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be is closed by the BIDDER at the time of filing of bid. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

- The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the bid process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the bid process or the contract, if already awarded, can be terminated for such reason.

5. Sanctions for Violations

5.1 Any breach of the aforesaid provisions by the BIDDER or anyone employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:

- To immediately call off the pre contract negotiations without assigning any

reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

- The Security Deposit / Performance Bank Guarantee (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason, therefore.
- To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.
- To recover all sums already paid by the BUYER with interest thereon at 1% higher than the prevailing Base Rate of a Scheduled Commercial Bank, while in case of a BIDDER from a country other than India with interest thereon at 1% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other services, such outstanding payment could also be utilized to recover the aforesaid sum and interest.
- To encash the Performance Bank Guarantee / Warranty Bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.
- To cancel all or any other Contracts with the BIDDER. The BIDDER shall· be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation / rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.
- To debar the BIDDER from participating in future bidding processes of the Bank for a minimum period of five years, which may be further extended at the discretion of the BUYER.
- To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or Agent or Broker with a view to securing the contract.
- In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.
- Forfeiture of Performance Bank Guarantee in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing

sanction for violation of this Pact.

5.2 The BUYER will be entitled to take all or any of the actions mentioned in Section 6.1 of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

5.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

6. Fall Clause

The BIDDER undertakes that it has not supplied / is not supplying similar product / services or sub-services in similar quantity during last one year from the date of issuance of this RFP, at a price lower than that offered in the present bid in respect of any other Ministry / Department of the Government of India or PSU or PSB and if it is found at any stage that similar product / services or sub-services was supplied by the BIDDER to any other Ministry / Department of the Government of India or a PSU or PSB at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

7. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

8. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

9. Other Legal Actions

The actions stipulated in this INTEGRITY PACT are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

10. Validity

The validity of this INTEGRITY PACT shall be from date of its signing and extend up to 12 months post last payment to the successful bidder as part of the overall contract whichever is later. In case BIDDER is unsuccessful, this INTEGRITY PACT shall expire after the appointment of the successful bidder. Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

11. The parties hereby sign this Integrity Pact at on

Reserve Bank of India BIDDER (legal entity)

Name of the Officer: Authorized Representative

Designation:

Department:

Witness Witness

Annex XVI- Non-Disclosure Agreement

Non-Disclosure Agreement

(On INR 100 stamp paper)

The Chief General Manager-in-Charge [Date]
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

[Salutation]

Confidentiality Undertaking

We acknowledge that during the course of bidding and in case of successful bidder, during the contract period for Request for Proposal for “Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India, we may have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to RBI and its business that is provided to us pursuant this Agreement. In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of our response to the RFP and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.

4. We shall not disclose or divulge any of the Confidential Information to any other client of [name of product vendor / implementation partner]
5. This Agreement shall not prohibit disclosure of Confidential Information:
    - To our partners/directors and employees who need to know such Confidential Information to assist with the bidding for RFP floated for Supply, Delivery, Installation, Support/ Services, Training, Testing, Commissioning, Warranty & Maintenance of in RBI;
    - With your prior written consent, such consent not to be unreasonably withheld;
    - To the extent that such disclosure is required by law;
    - To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply; and
    - To our professional advisers for the purposes of our seeking advice. Such professional advisors will be informed of the need to keep the information confidential.
6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:
    - For the purpose of a disclosure permitted by item 5 above; and
    - To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.
7. This Agreement shall not apply to Confidential Information that:
    - Is in the public domain at the time it is acquired by us;
    - Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us;
    - Is already in our possession prior to its disclosure to us; and
    - Is independently developed by us.
8. This Agreement shall continue perpetually unless and to the extent that you may release it in writing.
9. We acknowledge that the Confidential Information will not form the basis of any contract between you and us.
10. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.
11. We acknowledge that no failure or delay by you in exercising any right, power or privilege under this Agreement shall operate as a waiver thereof nor shall any

single or partial exercise thereof or the exercise of any other right, power, or privilege.

12. This Agreement shall be governed by and construed in accordance with Indian law and any dispute arising from it shall be subject to the exclusive jurisdiction of the Mumbai courts.

We have read this Agreement fully and confirm our agreement with its terms.

Yours sincerely

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Annex XVII - Self-Declaration on Sexual Harassment of Women at Workplace

(On letterhead of the bidder)

Compliance to Self-Declaration Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013

Strictly Private and Confidential

The Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

[Date]

[Salutation]

Sub: Request for Proposal for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India

Further to our proposal dated……., in response to - for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India (hereinafter referred to as "RFP") issued by Reserve Bank of India (hereinafter referred to as "RBI") we hereby covenant, warrant and confirm as follows:

Full compliance with the provisions of the "the sexual harassment of women at workplace (Prevention, Prohibition and Redressal) Act, 2013". In case of any complaint of sexual harassment against its employee within the premises of the Bank, the complaint will be filed before the Internal Complaints Committee constituted by the Bidder and the Bidder shall ensure appropriate action under said Act in respect to the complaint.

Any complaint of sexual harassment from any aggrieved employee of the Bidder against employee of the Bank shall be taken cognizance of by the Regional Complaints Committee constituted by the Bank.

The Bidder shall be responsible for any monetary compensation that may need to be paid in case the incident involves the employees of the Bidder, for instance any monetary relief to Bank's employee, if sexual violence by the employee of the Bidder is proved.

The Bidder shall be responsible for educating its employees about prevention of sexual harassment at workplace and related issues.

The Bidder shall provide a complete and updated list of its employees who are deployed within the Bank's premises.

Yours faithfully,

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Earnest Money Deposit

To,
The Chief General Manager-in-Charge
Department of Information Technology,
Reserve Bank of India,
Central Office,
Shahid Bhagat Singh Marg,
Mumbai 400 001

Dear Sir,

Request for Proposal for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Bank's Data Centres at Reserve Bank of India

WHEREAS The Reserve Bank of India, having its Central Office at Shahid Bhagat Singh Marg, Mumbai has invited RFP for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Bank's Data Centres at Reserve Bank of India on the terms and conditions mentioned in the tender documents.

1. It is one of the terms of invitation of tenders that the bidder shall furnish a Bank Guarantee for a sum of ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only) as Earnest Money Deposit.

2. M/s_____, (hereinafter called as Bidder), who are our constituents intend to submit their tender for the said work and have requested us to furnish guarantee to the Employer in respect of the said sum of ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only)

NOW THIS GUARANTEE WITNESSETH

1. We _____ (Bank) do hereby agree with and undertake to the Reserve Bank of India, their Successors, Assigns that in the event of the Reserve Bank of India coming to the conclusion that the Bidder have not performed their obligations under the said conditions of the tender or have committed a breach thereof, which conclusion shall be binding on us as well as the said Bidder, we shall on demand by the Reserve Bank of India, pay without demur to the Reserve Bank of India, a sum of rupees mentioned as EMD i.e., ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only) or any lower amount that may be demanded by the Reserve Bank of India. Our guarantee shall be treated as equivalent to the Earnest Money Deposit for the due performance of the obligations of the Bidder under the said Conditions, provided, however, that our liability against such sum shall not exceed the sum of EMD ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only)

2. We also agree to undertake and confirm that the sum not exceeding the EMD amount i.e., ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only) as aforesaid shall be paid by us without any demur or protest, merely on demand from the Reserve Bank of India on receipt of a notice in writing stating the amount is due to them and we shall not ask for any further proof or evidence and the notice from the Reserve Bank of India shall be conclusive and binding on us and shall not be questioned by us in any respect or manner whatsoever. We undertake to pay the amount claimed by the Reserve Bank of India within a period of one week from the date of receipt of the notice as aforesaid.

3. We confirm that our obligation to the Reserve Bank of India under this guarantee shall be independent of the agreement or agreements or other understandings between the Reserve Bank of India and the Bidder.

4. This guarantee shall not be revoked by us without prior consent in writing of the Reserve Bank of India.

5. We hereby further agree that -

a) Any forbearance or commission on the part of the Reserve Bank of India in enforcing the conditions of the said agreement or in compliance with any of the terms and conditions stipulated in the said tender and/or hereunder or granting of any time or showing of any indulgence by the Reserve Bank of India to the Bidder or any other matters in connection therewith shall not discharge us in any way our obligation under this guarantee. This guarantee shall be discharged only by the performance by the Bidders of their obligations and in the event of their failure to do so, by payment by us of the sum not exceeding Rs. ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only)

b) Our liability under these presents shall not exceed the sum of ₹ 10,98,64,377/- (Rupees Ten Crore Ninety Eight Lakh Sixty Four Thousand Three Hundred Seventy Seven only)

c) Our liability under this agreement shall not be affected by any infirmity or irregularity on the part of our said constituents in tendering for the said work or their obligations there under or by dissolution or change in the constitution of our said constituents.

d) This guarantee shall remain in force up to one year from the last date of submission of bid i.e., ----------, 2024 provided that if so desired by the Reserve Bank of India, this guarantee shall be renewed for a further period as may be indicated by them on the same terms and conditions as contained herein.

e) Our liability under this presents will terminate unless these presents are renewed as provided hereinabove on the day when our said constituents comply with their obligations, as to which a certificate in writing by the Reserve Bank of India alone is the conclusive proof whichever date is later. Unless a claim or suit or action is filed against us within six months from that date or any extended period, all the rights of the Reserve Bank of India against us under this guarantee shall be forfeited and we shall be released and discharged from all our obligations and liabilities hereunder.

Yours faithfully,

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

(NB: This guarantee will require stamp duty as applicable in the state, where it is executed and shall be signed by the official whose signature and authority shall be verified).

Performance Bank Guarantee Proforma

The Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

Dear Sir,

PEFORMANCE BANK GUARANTEE – Request for Proposal for Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India at Reserve Bank of India- Project B

WHEREAS

M/s. _____ (name of Bidder), a company registered under the Companies Act, 1956 / a partnership firm registered under the Partnership Act 1932, having its registered and corporate office at (address of the Bidder), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into an Contract/ Agreement dated …….. (hereinafter referred to as "the said Agreement") with you (Reserve Bank of India) for Supply, Installation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres at Reserve Bank of India, as detailed in the scope of work for the SI for the project in the RFP document for Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India- Project B, as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (…), Section (…), Chapter (…) of the said Agreement, our constituent is required to furnish a Performance Bank

Guarantee for an amount Rs……. (In words and figures), equivalent to 10% of the purchase order by the Bidder. This will be valid till the Stabilisation phase and payment associated with this milestone and submission of PBG for release of last payment instalments.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under:

I. In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/ not exceeding the sum of Rs…… (in words and figures) without any demur.

II. Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as afore-said and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

III. This Performance Bank Guarantee shall continue and hold good till the completion of the contract period subject to the terms and conditions in the said Agreement.

IV. We bind ourselves to pay the above said amount provided a claim or demand under this guarantee is made by RBI on us on or before completion of contract (date).

V. We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honour the same without demur.

VI. In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors

in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.

VII. We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of completion of the contract. (Date).

VIII. Any notice by way of demand or otherwise hereunder may be sent by special courier, fax, hand delivery, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

IX. If it is necessary to extend this Performance Bank Guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (Reserve Bank of India).

X. This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.

XI. Notwithstanding anything contained hereinabove, our liability under this Performance Bank Guarantee is restricted to Rs…… (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the date of completion of the contract. (Date).

XII. We hereby confirm that we have the power/s to issue this Guarantee in your favour under the Memorandum and Articles of Association/ Constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favour.

2. We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Agreement, would

not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee. Notwithstanding anything contained herein:

I. Our liability under this Performance Bank Guarantee shall not exceed Rs…….. (in words and figure);

II. This Performance Bank Guarantee shall be valid only up to …….. (Date); and

III. We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before the date of completion of the contract. (Date).

This Performance Bank Guarantee must be returned to the bank upon its expiry. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated ……. this …….day……. 2025. Yours faithfully,

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Annex XX- Compliance Certificate of Commercial Bid

Compliance Certificate of Commercial Bid

(On letterhead of the Bidder)

Date

The Chief General Manager-in-Charge
Department of Information Technology
Reserve Bank of India
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai-400 001

Dear Sir,

Subject: Bid dated MMMM, DD, YYYY COMMERCIAL BID for - for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India.

Having examined the Bid Document, we, the undersigned, offer to supply, deliver, implement, and commission ALL the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Bid Documents for a total bid price of:

Indian Rupees in words and figures.

We attach hereto the Bid Commercial Response as required by the Bid document, which constitutes our bid.

We undertake, if our Bid is accepted, to adhere to the implementation plan put forward in our Bid Response or such adjusted plan as may subsequently be mutually agreed between us and the Reserve Bank of India or its appointed representatives.

We hereby confirm the prices quoted by us are reasonable and as per industry standards.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company

/firm/organization and empowered to sign this document as well as such other documents which may be required in this connection.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely “Prevention of Corruption Act 1988”.

Dated this ……. Day of ……..2025

……. …….

(Signature) (In the capacity of)

Duly authorized to sign the Bid Response for and on behalf of:

……
……
……
……

(Name and address of Bidding Company)

Seal/Stamp of Bidder

Witness name:

……

Witness address:

……

……...

Witness signature:

……

Annex XXI - Letter of Authority

Letter of Authority

(This 'Letter of Authority' should be issued on the letterhead of the OEM)

Place:

Date:

The Chief General Manager-in-Charge
Department of Information Technology,
Central Office, Reserve Bank of India,
14th Floor, Central Office Building,
Shahid Bhagat Singh Road,
Mumbai – 400 001.

Dear Sir,

Subject: Letter of Authority

We have been approached by M/s_____ in connection with your tender name _____No._____dated_____.

We confirm having offered to them the software/ hardware in line with your requirement outlined in the RFP for "Supply, Installation, Implementation, Integration, Maintenance and Facilities Management Services for IT Security Infrastructure at Data Centres of Reserve Bank of India.

Our offer to them is for the following software/hardware for which we are the OEM and having back-to-back support agreement with the bidder to meet the required SLA as per RFP.

1._____
2._____
3._____
4._____
5._____

The authorized agency would independently support and service the above-mentioned software / hardware during the contract period.

_____

(Signature of Authorized Signatory)

<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF

<NAME OF THE APPLICANT ORGANISATION>

Annex XXII - Acceptance Certificate

(**To be submitted by the Successful Bidder on supply, installation, testing and commissioning of Security Infrastructure at Bank's Data Centres**)

No. Date:

M/s. ……

……

Sub: Certificate of Delivery/Installation/Testing and Commissioning of IT Security Infrastructure at Bank's Data Centres

This is to certify that the Systems/Solution as detailed below have been received in good condition along with all the standard and other accessories (subject to remarks in para No.3) in accordance with the Contract/Specifications. The same have been received at the office location in good condition subject to verification.

1) The delivered equipment/Solutions have been installed and commissioned successfully.

a) Contract No. _____ dated _____

Sr. No.	Description	Qty	Delivery dt.	Installation dt.

2) Details of services not yet supplied and recoveries to be made on that account:

Sr. No.	Description	Amount to be recovered

3) The Contractor has fulfilled his contractual obligations satisfactorily*

OR

The Contractor has failed to fulfil his contractual obligations with regard to the following:

a) ……

b) ……

4) The amount of recovery on account of non-render of Services /Systems is given under Para No._____.

5) The amount of recovery on account of failure of the Contractor to meet his contractual obligations is as indicated in endorsement of the letter.

Signature: _____

Name : _____

Designation: _____

Strike out whichever is not applicable.

Explanatory notes for filing up the certificates:

(a) It has adhered to the time schedule specified in the contract in dispatching / installing the systems/ manuals pursuant to Technical Specifications.

(b) He has supervised the commissioning of the services in time i.e., within the period specified in the Contract from the date of intimation by the Purchaser in respect of the installation of the system.

(c) Training of the personnel has been done by the bidder as specified in the Contract.

(d) In the event of Manuals having not been supplied or installation and commissioning of the Services having been delayed on account of the Contractor, the extent of delay should always be mentioned.

Annex XXIII - Acceptance Criteria- Broad Parameters

The indicative list of Broad parameters for acceptance test of the solution is as follows:

S. No.	Acceptance Criteria
	Firewalls
1.	One successful failover exercise (High Availability) & DC-DR Failover Configuration and Testing must be demonstrated by the SI.
2.	50% of required throughput for NGFW should be available for acceptance test (approx. average of one-month post implementation) with balance headroom for future increase in the requirement assuming straight line 20% yearly growth.
3.	Basic Configuration such as License Activation, IP, Interface and VLAN, NTP, SNMP, SMTP and DNS configuration as per the final agreed design
4.	Integration with SOC solutions such as SIEM, SOAR and PIM, etc.
5.	ACL Policies as per the Pre-Requisites defined during the design stage - Up to 25 Policies
6.	Enable and Configure Proxy pac files and URL Filtering Profiles - Up to 5 Profiles (for External Firewall only).
7.	Enable and Configure IPS Security Policies - Up to 10 Policies
8.	Central Management Dashboard Configuration - Up to 5 Standard or Customised Widgets
	WAF
1.	Application Security policies for applications need to be created and associated with application VIP – up to 5 applications
2.	Bot profile for applications need to be created and associated with application VIP – up to 5 applications
3.	Security logging profiles should be created and associated with application for event logging. Up to 5 applications
4.	High level accuracy signatures need to be put in block mode for 5 applications.
5.	Medium and Low-level signatures need to be put in block mode for 2 applications.

6.	Bidder shall configure File Types (Up to 15 per policy), URLs (Up to 15 per policy), Parameters (Up to 15 per policy), and Headers (Up to 15 headers, cookies or hostnames per policy).
7.	Enable BOT and DDOS profiles for standard signatures
8.	Integration with SIEM, PIM, SNMP, SMTP as applicable
9.	Demonstrate configuration of Real-time updates of latest signatures as per best practices to download frequent updates.
10.	Security reports based on top attacks/violations
11.	For WAF Implementation in existing data Centres, in addition to already existing all of the above test criteria, OEM & Bidder shall ensure that Application Security policies, Bot Profile, Security logging profiles for event logging, High-Medium and Low-level accuracy signatures for applications need to be created and associated with application VIP for UAT of all applications in existing three DCs: PDC, ODC & DRDC
SSLO	
1.	Create inbound topology based on orchestration policies with desired service chains.
2.	Configure security devices in service chain and configure in desired topologies. Up to 3 devices
3.	Configure SSL rules/policies to intercept SSL traffic.
4.	Create SSL profiles for atleast 5 applications to intercept SSL traffic for inspection.
5.	Create TCP listener (non-HTTP) to accept traffic for inspection.
6.	Create UDP listener to accept traffic for inspection.
7.	Create per request policies to be called in topologies for orchestration of traffic.
8.	Showcase the report on top usage by apps, top protocols, etc.
9.	Integration with SIEM, PIM, SNMP, SMTP as applicable
SLB	
1.	Onboard 5 applications for server load balancing
2.	Configure HTTP profiles per applications.
3.	Configure desire load balancing methods based on origin server requirement

4.	Configure SNAT per application.
5.	Integration with SIEM, PIM, SNMP, SMTP as applicable
Anti-DDoS	
1.	Implementation of DDoS Solution as per the agreed design
2.	Integration with applicable 3rd party solutions such as AAA, PIM, SIEM, TIP and SMTP as agreed with Bank
3.	Licenses and module activation as per the subscription
4.	Standard Monitoring and blocking profiles for volumetric attack – up to 5 policies
5.	Configuration and demonstration of System alerts – thresholds and triggers
6.	Configuration of device protection information – filters, traffic profile, baselines
7.	Standard base backups, system maintenance
GSLB	
1.	Ensure efficient traffic distribution across multiple geographic locations.
2.	Automatic rerouting of traffic during server or data centre failure.
3.	Creation of DNS records for application published from respective data centres.
4.	Enable DNS DDOS protection for inbound DNS traffic
5.	Report of top DNS queries.
6.	Report of statistical information of inbound and outbound traffic through Link Load Balancer.
7.	Integration with SIEM, PIM, SNMP, SMTP as applicable
Threat Intelligence Feeds	
1.	Integration of Threat Intel feeds with SOAR and TIP solution along with demonstration of mandatory specifications mentioned under Annex III.

ARUN SHARMA

Digitally signed by ARUN SHARMA
Date: 2025.06.09 18:10:12 +05'30'