TABLE OF CONTENTS

1 DISCLAIMER

1.1 Though adequate care has been taken in the preparation of this *Request for Proposal* Document, the Bidder should satisfy himself that the Document is complete in all respects. Intimation of discrepancy, if any, should be given to the below mentioned office latest by the date mentioned in Sec.5.7. If this office receives no intimation by the date mentioned in Section 5.7, it shall be deemed that the Bidder is satisfied that the *Request for Proposal* Document is complete in all respects.

Member Secretary
Maharashtra Pollution Control Board
Kalpataru Point, 3rd floor,
Opp. Cine Planet Cinema, Sion Circle
Sion (E), MUMBAI – 22
Ph: 022-24014701
Fax: 022-24024068

1.2 Neither **MPCB,** nor their employees or consultants make any representation or warranty as to the accuracy, reliability or completeness of the information in this RFP nor is it possible for **MPCB** to consider the financial situation and particular needs of each party who reads or uses this RFP. **MPCB** recognizes the fact that certain prospective Bidders may have a better knowledge of the Project than others and thus encourages all prospective Bidders to conduct their own investigations and analysis and check the accuracy, reliability and completeness of the information in this RFP and obtain independent advice from appropriate sources.

1.3 Neither **MPCB** nor their employees or consultants will have any liability to any prospective Bidder or any other person under the law of contract, tort, the principles of restitution or unjust enrichment or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with anything contained in this RFP, any matter deemed to form part of this RFP, the award of the Project, the information and any other information supplied by or on behalf of **MPCB** or their employees, any consultants or otherwise arising in any way from the selection process for the Project.

1.4 **MPCB** reserves the right to reject any or all of the Bids submitted in response to this *Request for Proposal* at any stage without assigning any reasons whatsoever.

1.5 **MPCB** reserves the right to change any or all of the provisions of this *Request for Proposal.* Such changes would be intimated to all parties procuring this *Request for Proposal.*

2 LIST OF ABBREVIATIONS

MPCB	Maharashtra Pollution Control Board
RO	Regional Office, MPCB
SRO	Sub-Regional Office, MPCB
HO	Head Office, MPCB
RFP	Request for Proposal
IMIS	Integrated Management Information System
NOC	Network Operations Centre
SOC	Security Operations Centre
OEM	Original Equipment Manufacturer
LAN	Local Area Network
WAN	Wide Area Network
PBG	Performance Bank Guarantee
LoA	Letter of Award
SP	Solution Provider
SI	System Integrator
MPLS	Multi Protocol Label Switching
VPN	Virtual Private Network
Mbps	Mega Bits per Second
KBps	Kilo Byte per Second
MB	Mega Bytes
GB	Giga Bytes
TB	Tera Bytes
Gbps	Giga Bits per Second
MBps	Mega Bytes per Second
GBps	Giga Bytes per Second
VM	Virtual Machine
IPS	Intrusion Prevention System
IDS	Intruder Detection System
ISP	Internet Service Provider

3 DEFINITIONS

3.1 BID

The bids submitted by the prospective Bidders in response to this Request for Proposal Document issued by **MPCB.**

3.2 BIDDER

Bidding Firm / Company that has submitted a Bid in response to this Request for Proposal Document.

3.3 DOCUMENT / BID DOCUMENT

This Request for Proposal Document.

3.4 PROJECT

To select a Solution Provider (SP) for **Supply, Installation, Commissioning and Support of Integrated IT Security solution** at MPCB HQ in State of Maharashtra.

3.5 REQUEST FOR PROPOSAL

This Document, being issued to the prospective Bidders, inviting their Bids.

3.6 RESPONSIVE BIDDER

Responsive Bidder is the bidder whose bid is found responsive after evaluation of the Bid as outlined in Section 5.2.

3.7 INTEGRATED SECURITY SOLUTION

An integrated IT security solution which consists of minimum three of the following five components : Firewall, Sandboxing solution, Email security solution, SIEM, Web Application Firewall

4 PROJECT CONCEPT & STRUCTURE

4.1 BACKGROUND

Maharashtra Pollution Control Board (MPCB) is an organization under the Ministry of Environment and Forests (MoEF), Government of Maharashtra. The Board is responsible for ensuring that all norms under the Pollution Control Act, as stated by the Ministry, are adhered to by all relevant establishments in Maharashtra, which can, through their operations or processes, influence the natural environmental conditions.

To cater to its citizen charter and as a part of Maharashtra States ”ease of business” initiative, the Board has developed a comprehensive IT strategy. The IT strategy includes the Applications, Core Infrastructure, Connectivity of all the offices (RO, SRO, Laboratory, HO), Data Centre, Disaster Recovery for Business continuity and Governance. An amalgamation of all these components is a strong e-governance platform and is known as Integrated Management Information System (IMIS).

The Board has already deployed IT security infrastructure to address and counter various IT security threats, The details of th same are mentioned briefly in the section 4.2 and elaborated further in Annexure -1. The board acknowledges the rapidly changing IT trends and the need for a dynamic and proactive security infrastructure. Hence, the Board is in the process of revamp and upgrade of the current IT security infrastructure with better features and capabilities.

4.2 CURRENT INFRASTRUCUTRE

MPCB has an on-site Data Centre facility which has been recently modernized, The modernized infrastructure running on Virtualized Platform is robust, fail-safe and scalable. There are various applications which are accessed by the MPCB users in their regional and sub-regional offices (RO and SRO) and Laboratories across Maharashtra. These offices are connected through MPLS VPN. The Infrastructure is protected by an integrated security infrastructure consisting of Firewall, Sandboxing Solution, Email security Solution and Logging and recording solution.

The details of the relevant current infrastructure are given at Annexure -1 for the convenience of the bidders.

4.3 OBJECTIVE OF RFP

The RFP intends to select System Integrator / Solution Provider having the requisite experience, resources and capabilities which will provide and commission a suitable IT Security Solution.

4.4 BRIEF SCOPE OF WORK

The broad scope is defined below.

1. Supply of appliances and software fulfilling the requirements of the proposed Security Solution along with additional software required, if any, with provision of version upgrades/ patches as per specification given in RFP.
2. Installation, implementation & maintenance of the Security Solution
3. Provision of all licenses/subscriptions
4. Study / Create Integrated IT Security Solution security policies
5. Migration of existing Security policies
6. Performance tuning
7. Rule/signature tuning
8. Comprehensive onsite warranty of 3 year
9. Training and Documentation

4.5 PROJECT COMPLETION SCHEDULE

The SP is required to complete the supply, installation, commissioning, policy creation, implementation and testing of the Solution at MPCB Data Center within NINE (09) week of receipt of the LoA.

5 DESCRIPTION OF THE SELECTION PROCESS

5.1 SUBMISSION OF BIDS

The submission of Bids electronically by interested bidders in response to the Request for Proposal should be through e-Tender system only as mentioned in **Annexure 5**. The Bids will be

Envelope 1 / Cover 1: Technical Bid
Envelope 2 / Cover 2: Price Bid.

5.2 RESPONSIVENESS OF BID

The Bids submitted by Bidders shall be initially scrutinized to establish "Responsiveness". A Bid may be deemed "Non-responsive" if it does not satisfy any of the following conditions:

1. It is not received by the due time & date specified in the section 5.7
2. It is not accompanied by payment towards price of the RFP
3. It does not include EMD as stipulated in the RFP
4. It does not include sufficient information for it to be evaluated and/or is not in the formats specified.
5. It is not signed and / or sealed in the manner and to the extent indicated in Section 6 of this RFP Document.
6. It does not conform to the terms and conditions mentioned in the RFP

The Bids of Responsive Bidders shall be evaluated in the following two steps.

5.3 STEP 1 (COVER 1) – TECHNICAL BID EVALUATION

In the first step, MPCB will evaluate the information submitted by the Bidder in Cover 1 of the Bid. Bids of only the responsive Bidders shall be considered for the subsequent technical evaluation. The evaluation criteria for assessment of the Technical Bid are described in Section-7. MPCB, on a written demand, will return unopened, the Cover 2 of the Bid, viz: the Price Bid, to the Bidders whose Bids are not responsive.

5.4 STEP 2 (COVER 2) – PRICE BID AND PRICE BID EVALUATION

The Price Bid would seek to identify the Bidder making the most competitive price offer to MPCB. The evaluation criteria for assessment of the Price Bid are described in Section -8. The format for the Price Bid is specified in **Annexure - 4**

A ranked list of Bidders based on the results of the evaluation, as detailed in Section-8 of this Document, would be presented. The top ranked Bidder will be designated the Successful Bidder. MPCB is not bound to award a LoA to the lowest price bidder.

5.5 AWARD OF LoA

Successful Bidder would be given a Letter of Award (LoA) stipulating the conditions under which the bid has been qualified as the Successful Bid.

5.6 SIGNING OF ORDER ACCEPTANCE

The Successful Bidder would sign a copy of the Purchase / Work Order as a token of acceptance of the same.

5.7 SCHEDULE OF ACTIVITIES

Sr. No.	ACTIVITY	Date
1.	Date of Start of Sale of RFP document	17th September 2020
2.	Date of End of Sale of RFP document	30th September 2020
3.	Last date for receipt of requests for clarifications	25th September 2020
4.	Pre-bid Conference	28th September 2020 15:00 Hrs
5.	Bid Submission Last dates	09th Oct 2020 17:00 Hrs
6.	Time and Date of Opening of Cover-1	13th Oct 2020 15:00 Hrs

Bidders are also requested to read Annexure – 5 for detailed schedule of activities related to this RFP and bid submission process.

In order to enable MPCB to meet the target dates, Bidders are expected to respond expeditiously to clarifications, if any, requested during the evaluation process. MPCB shall adhere to the above schedule to the extent possible. MPCB, however, reserves the right to modify the same. Intimation to this effect shall be given to all Bidders.

6 PROCEDURES TO BE FOLLOWED

6.1 ENQUIRIES & CLARIFICATIONS

Enquiries, if any, should be addressed to:

Member Secretary
Maharashtra Pollution Control Board
Kalpataru Point, 3rd floor,
Opp. Cine Planet Cinema,Sion Circle,
Sion (E), MUMBAI – 400 022
Ph: 022-24014701
Fax: 022-24024068
Email : eic@mpcb.gov.in

All queries that are received on or before the date mentioned in Section 5.7 shall be addressed by MPCB in writing. MPCB shall aggregate all such queries, without specifying the source and shall prepare a response, which shall be distributed to all parties who have procured the Request for Proposal Document. It may be noted that queries in writing would be entertained only from those parties who have procured this Document.

Request for clarifications received from prospective bidders who have not paid the fee for the RFP document as defined in 6.6.1, will not be answered. Such bidders will not be allowed to attend the pre bid meeting and also to bid.

Request for clarifications received after the last date mentioned in Section 5.7, may not be addressed. Decision of the Board in the matter will be final.

The prospective Bidders shall submit the queries only in the format given below:

Sr. No	RFP Page No	RFP Clause No	Description in RFP	Clarification Sought	Additional Remark (if any)

6.2 SUBMISSION OF THE BID

1. Cover 1 – Technical Bid

   The information to be submitted by the Bidders as Cover 1 of their Bids is described in Section 7 and Annexure 5.

2. Cover 2 – Price Bid

The Information to be submitted by the Bidders in the Price Bid (Cover 2) is described in Section 8 and Annexure 5.

3. Submission of the Bid

   The Bidders are requested to follow the Bid submission process which is detailed in Annexure 5 as per the schedule elaborated in Section 5.7 and Annexure 5.

   MPCB shall not be responsible for any delay in submission of the Bids. Any Bid received by MPCB after the due date for submission of the Bids stipulated in Section 5.7 and Annexure 5, will not be opened..

6.3 INITIALING OF THE BIDS

As prescribed in the Annexure 5, under this e-tender process the bids should be digitally signed. Any testimonials being presented should be self-attested before uploading.

6.4 INSTRUCTIONS TO BIDDERS

All Bidders should note the following:

1. Bids received after the scheduled time will not be accepted by MPCB under any circumstances. MPCB will not be responsible for any delay for any reason whatsoever.

2. Bid once submitted will be treated, as final and no further correspondence will be entertained on this. No Bids will be modified after the deadline for submission of Bids.

3. Bids that are incomplete in any respect or those that are not consistent with the requirements as specified in this *Request for Proposal* or those that do not contain the Covering Letter and other documentation as per the specified formats may be considered non-responsive and may be liable for rejection.

4. Strict adherence to formats, wherever specified, is required. Non-adherence to formats may be a ground for declaring the Bid non-responsive.

5. All communication and information should be provided in writing and in the English language only.

6. The metric system shall be followed for units.

7. The price quotations for the bid should be denominated in Indian Rupees.

8. All communication and information provided should be legible, and wherever the information is given in figures, the same should also be mentioned in words.

9. Arithmetical errors will be rectified as follows –

   a. If there is a discrepancy between the unit price and the total price that is obtained by multiplying quantities, the unit price will prevail
   b. In case of discrepancy between grand total obtained by adding various line item totals & the grand amount stated in words, the grand total will be recalculated and the same will be taken as correct.
   c. **The price bid will be treated as inconsistent & non-responsive, in case if more than one type of discrepancy is observed in the price bid. Such price bid/s will be rejected summarily and considered as intentional misrepresentation and the EMD will be forfeited.**

10. MPCB reserves the right to seek additional information from the Bidders, if found necessary, during the course of evaluation of the Bid. Non-submission, incomplete submission or delayed submission of such additional information or clarifications sought by MPCB, may be a ground for rejecting the Bid.

11. The Bids shall be evaluated as per the criteria specified in this RFP Document. However, within the broad framework of the evaluation parameters as stated in this Request for Proposal, MPCB reserves the right to make modifications to the stated evaluation criteria, which would be uniformly applied across all the Bidders.

12. The Bidder should designate one person (“Contact Person” and “Authorized Representative and Signatory”) authorized to represent the Bidder in its dealings with MPCB. This designated person should hold the Power of Attorney and be authorized to perform all tasks including but not limited to providing information, responding to enquiries, entering into contractual commitments on behalf of the Bidder etc. The Covering Letter submitted by the Bidder shall be signed by the Authorized Signatory and shall bear the stamp of the entity thereof.

13. The Bid (and any additional information requested subsequently) shall also bear the initials of the Authorized Signatory and stamp of the entity thereof on each page of the Bid.

14. MPCB reserves the right to reject any or all of the Bids without assigning any reason whatsoever

15. Conditional bids may be summarily rejected.

16. Mere submission of information does not entitle the Bidder to meet an eligibility criterion. MPCB reserves the right to vet and verify any or all information submitted by the Bidder.

17. If any claim made or information provided by the Bidder in the Bid or any information provided by the Bidder in response to any subsequent query by MPCB, is found to be incorrect or is a material misrepresentation of facts, then the Bid will be liable for rejection and the Bid Security will be forfeited. Mere clerical errors or bonafide mistakes may be treated as an exception at the sole discretion of MPCB and if MPCB is adequately satisfied.

18. The Bidder shall be responsible for all the costs associated with the preparation of the Bid. MPCB shall not be responsible in any way for such costs, regardless of the conduct or outcome of this process.

19. MPCB may, at its discretion, extend this deadline for submission of Bids by amending the RFP which will be intimated through MPCB website, in which case all rights and obligations of MPCB and bidder will thereafter be subject to the deadline as extended.

6.5 VALIDITY OF THE PRICE BID

Each Bid shall indicate that it is a firm and irrevocable offer, and shall remain valid and open for a period of not less than 180 days.

Non-adherence to this requirement and other terms stipulated in the RFP document may be a ground for declaring the Bid as non-responsive. However, MPCB may solicit the Bidder’s consent for extension of the period of validity if the Bidder agrees to reasonably consider such a request. The request and response shall be in writing. A Bidder accepting MPCB’s request for extension of validity shall not be permitted to modify his Bid in any other respect.

MPCB, reserves the right to vary the quantities by ± 25% of the proposed quantities, add or remove locations, during the validity period of the contract. For any such changes made in quantities and the locations, the price mentioned only in the contract shall be considered. No revision in the prices, especially upwards, will be granted in the contracted prices.

6.6 FEES AND DEPOSITS TO BE PAID BY THE BIDDERS

6.6.1 Fees for Request for Proposal (RFP) document

The RFP can be purchased by making a payment (non-refundable) of **Rs. 5,000.00 (Rs. Five Thousand only)** through online payment. Please refer Annexure 5 of this document for the payment methodology.

It is mandatory for the bidders to display the proof of purchase of the RFP document to attend the pre-bid meeting. Prospective bidder failing to pay the fee for the RFP during the sale of RFP document will neither be allowed to attend the pre-bid meeting nor will his bid be accepted.

6.6.2 Earnest Money Deposit (EMD)

Bidders are required to submit a Earnest Money deposit (EMD) for an amount of **Rs. 3,00,000.00 (Rupees Three Lakh Only)** Please refer Annexure 5 for the payment of the same. Bids of the bidders who have not paid the EMD as stipulated in this RFP, will be rejected by MPCB as non-responsive. No exemptions to this clause will be allowed.

MPCB shall reserve the right to forfeit the Bidder's EMD under the following circumstances:

1. If the Bidder withdraws his Bid at any time during the stipulated period of Bid validity as per Section 9.1 (or as may be extended).

2. If the Bidder, for the period of Bid validity:

   i) in MPCB's opinion, commits a material breach of any of the terms and / or conditions contained in the RFP Document and / or subsequent communication from MPCB in this regard and / or
   ii) fails or refuses to execute the LoA (in the event of the award of the Project to it) and/or
   iii) fails or refuses to furnish the Performance Guarantee within the stipulated time

3. Any claim made or information provided by the Bidder in the Bid or any information provided by the Bidder in response to any subsequent query by MPCB, is found to be incorrect or is a material misrepresentation of facts

In the event that any Bid is non-responsive or rejected after technical evaluation, the EMD of such Bidders shall be refunded with the unopened Cover – 2 of their Bid.

In respect of the bids after Technical Evaluation and eligible for price bid evaluation, the EMD of the unsuccessful Bidders (after opening of Cover 2) can cease to be in force after 60 days following the announcement of award of the Project to the Successful Bidder through the issue of the LoA for the same. The EMD of the Successful Bidder will be returned only on submission of SPBG that Successful Bidder will provide at the time of signing Order acceptance & the SLA. EMD of the unsuccessful bidders will be returned after 45 days of award of contract.

7 SUBMISSION OF TECHNICAL BID: COVER - 1

7.1 CRITERIA FOR MINIMUM ELIGIBILITY AND BID RESPONSIVENESS:

The Bidder shall fulfill all of the following Minimum Eligibility Criteria to participate in the bidding process. The Bidder should provide necessary documentary evidences of compliance as follows. Failure to do so for any of the Criteria mentioned below shall result in disqualification of the Bidder.

1. The Bidder should be public or private limited company registered / incorporated under The Companies Act, 1956, and in business of IT System Integration and providing IT Security Services / Integrated Security Solutions (i.e. in the area of implementation of Firewalls / UTM / IPS/ IT Security and solutions) for minimum FIVE (5) years would be eligible to bid for the Project. No consortiums allowed.

2. The Bidder should be profitable for each of the past three financial years ending 31st March 2020

3. The Bidder should have ISO 9000 certificate valid as on date of bidding.

4. The Bidder should have officially purchased the RFP by paying the necessary fees as per section 6.6.1 and Annexure 5 of the RFP.

5. The Bidder should submit the EMD as stipulated in section 6.6.2 and **Annexure 5**

6. The Bidder should have executed (completed) at least one project for Integrated Security Solution of minimum value of Rs.1 Crore in the past three years that is after 1st April 2017. Such project should have at least three of the following five components - Firewall, Sandboxing solution, Email security solution, SIEM, Web Application Firewall.

7. The Bidder should be authorized by Manufacturers / OEM to supply, install and support the products required by MPCB being proposed for this RFP The same should be documented in the format for Manufacturer's Authorisation Form (MAF) in Exhibit-3.

8. The product should be an OEM product listed in the Magic Quadrant as per the 2019 Gartner Reports / NSS labs report and should have 100% compliance to all the technical Specifications mentioned in Annexure 2. The bidder should submit a declaration to that effect by the Manufacturer / OEM as per Exhibit 3.

9. Bidder should have office in Mumbai.

7.2 COVER 1: INFORMATION FORMATS

Bidders are required to organize Cover-1 as per the following checklist -

Cover 1	Compliance to Minimum Eligibility Criteria and Technical Bid
Section 1	a) Covering Letter as per the format specified in EXHIBIT 1 b) Attested copy of Power of Attorney c) Certificate of incorporation / registration d) Certificate from CA for compliance to section 7.1 (2) e) Certificate in compliance to section 7.1 (3) f) Proof of Purchase of the RFP document for 7.1.(4) g) EMD as per section 6.6.2 h) Copy of order / completion certificate as per section 7.1 (6) i) Manufacturer’s authorization form and declaration from OEM as per EXHIBIT 3 in compliance of section 7.1 (6) j) Declaration with details of office locations, contact personnel, infrastructure, ownership / rent agreement for the office in compliance to 7.1 (9)
Section 2	a) Documentary Proofs as testimony for Evaluation of Technical bids as per criteria listed in Section 7.4.1 b) Necessary technical brochure / literature, duly highlighting the relevant features / specifications required by MPCB

7.3 TECHNICAL BID - COVER 1

The Cover 1 submission will also include Technical Bid of the bidder.

1. The technical bid should be in line with the scope of work as described in the Section 4 and Annexure 3.

2. Technical literature for the product and services, covering full technical specifications, principal of operation, design features, test & monitoring facilities, description of operation.

3. The bid should have all relevant testimonials, so as to ensure they score maximum marks under the evaluation system defined in section 7.4.1

7.4 TECHNICAL BID: EVALUATION CRITERIA & PROCESS

The Bidder shall necessarily submit in Cover 1 of the Bid Document, the Technical Bid detailing his credentials for executing this project and the highlights of the equipment & services offered by him with respect to scope of work defined in the Bid Document and the benefits that would accrue to MPCB. The Screening Committee appointed for this purpose will do this evaluation. The Technical Bid will contain all the information required to evaluate the bidder’s suitability to MPCB for the purpose of this project.

The guidelines for evaluation have been designed to facilitate the objective evaluation of the Technical Bid submitted by the bidder. The information furnished by the bidders in the technical bid shall be the basis for this evaluation. In case any of the information is not made available, the Committee will assign zero (0) marks to that item.

While evaluating the Technical Bid, MPCB reserves the right to seek clarifications from the Bidders. Bidders shall be required to furnish such clarifications in a timely manner.

MPCB also reserves the right to seek additions, modifications and other changes to the submitted Bid. Bidders shall be required to furnish such additions / modifications / other changes in a timely manner.

7.4.1 Evaluation of Technical Bid

The technical evaluation of the bidders will be done based on the criteria and marking system as specified as follows:

Sr. No.	Criteria	Graded Marks	Max. Marks	Testimonial to be presented
1	**Financial Capability**		**5**	
	Average Turnover (AT) of the organisation for past three years ending on 31st March '20			Certificate from CA
	AT < Rs. 2.00 cr but ≥ Rs. 1.00 cr	**1**		
	AT < Rs. 5.00 cr but ≥ Rs. 2.00 cr	**2**		
	AT ≥ Rs. 5.00 crores	**5**		
2	**Past Performance (Orders executed in past 3 years ending 31st March 2020)**		**40**	
a	Order for supply, implementation and commissioning of Integrated Security solution to Govt organisation (state / central / urban local bodies / PSUs)	**10**		Copies of the orders executed in the designated period
	2 Marks per order			
b	Order for supply, implementation and commissioning of Integrated Security solution in the organisation where organisation have offices at multiple locations (min 5) connected over WAN	**10**		
	5 Marks per order			
c	Order for Remote Security Support through SOC	**5**		
	2.5 Marks per order			
d	Orders for supply, implementation and commissioning of Integrated Security solution (Firewall / UTM / IDS solution) where each order has users > 500	**10**		
	2 Marks per order			
e	Orders for offering any of the following services (1) threat and vulnerability management (2) SIEM (3) identity access management (4) cloud security.	**5**		
	2.5 Marks per order			
3	**Certifications and certified professionals**		**45**	
a	ISO 20000 certification for the organisation	**5**		Certificate valid at time of bidding
b	ISO 27000 certification for the organisation	**5**		
c	Having a Security Operating Center to facilitate Remote security support with SLA	**5**		Detailed writeup @ resources and infrastructure deployed with a declaration and address proof
d	Certified resources at-least for SIX (6) months on company roll (5 marks per each resource)	**30**		Declaration by bidder on company letterhead and Copies of Certificates
	OEM Certified Resources (appliance)	**15**		
	CEH / CPTE , CISSP / CISA -M / CCNA Security Resources	**15**		
4	**Presentation by the Bidders**		**10**	Presentation by bidders on methodology
	TOTAL MARKS		**100**	

CISSP - Certified Information Systems Security Professional
CISA / M - Certified Information Security Auditor / Manager
CEH - Certified Ethical Hacker
CPTE - Certified Penetration Testing Engineer
CCNA Security - Certified CISCO Network Administrator with Security Specialisation

Each responsive Bid will be attributed a **technical score denoted by symbol "S(t)" .** The technical score shall be out of a maximum of 100 marks.

If in MPCB's opinion, the Technical Bid does not meet the minimum technical specifications & service requirements or is otherwise materially deficient / inconsistent in any other aspect; the Bid shall be declared Technically Evaluated & Non-Responsive and shall not be considered for further evaluation.

After technical evaluation, MPCB will rank the bidders in descending order of their technical scores with the top ranked bidder having the highest technical score. If any bidder is found to be technically inadequate to the requirements of MPCB, i.e. if the technical marks are lower than **75**, then that bidder's bid would be deemed non-responsive for further evaluation and would not be considered further in the bidding process.

If in case, after technical evaluation, only one bidder is found to be responsive & eligible, i.e. if the technical marks of only one bidder are more than or equal to 80, the Board will decide an acceptable price band and open Price Bid of the only eligible bidder. If the price bid of the bidder falls within the price band specified by the Board, the bidder will be declared as the SUCCESSFUL BIDDER.

8 EVALUATION OF PRICE BID: COVER 2

8.1 PRICE BID PARAMETERS

Bidders are required to offer their best prices in terms of cost of the Equipment & Services including all taxes and levies as on the last date of submission of bid (detailed break-up of all applicable taxes and levies over and above the quoted price should be mentioned)

8.2 EVALUATION OF PRICE BIDS AND RANKING

The price bids of only technically successful bidders whose technical Bids have been awarded **75** or more marks by the Committee will be opened.

The evaluation will carried out if Price bids are complete and computationally correct. For the purpose of evaluation, only the Grand Total Price will be considered. Lowest Price bid (denoted by symbol "P (m)") will be allotted a Price score of 100 marks. The Price score will be denoted by the symbol "S (p)". The Price score of other bidders will be computed by measuring the respective Price bids against the lowest bid.

These Price scores will be computed as: S (p) = 100 * (P (m) / P) where P is the Price bid of the bidder whose Price score is being calculated. The Price score shall be out of a maximum of 100 marks.

8.3 COMPUTING THE FINAL SCORE

The composite score is a weighted average of the Technical and Price Scores. The weightages of the Technical vis-à-vis the Price score is 0.70 of the Technical score and 0.30 of the Price score. The composite score (S) will be derived using following formula:

$$S = (S(t) * 0.70) + (S (p) * 0.30) .$$

Thus the composite score shall be out of a maximum of 100 marks.

The responsive bidders will be ranked in descending order according to the composite score as calculated based on the above formula. The highest-ranking vendor as per the composite score will be selected. However in order to ensure that MPCB gets best solution in technical terms, MPCB reserves the right to enter into negotiation with bidder having highest technical score and place order with this bidder at a suitable price.

8.4 AWARD CRITERIA

Final choice of MPCB to award this project to a suitable bidder to execute this project shall be made on the basis of composite scoring arrived as per formula mentioned above.

8.5 NOTIFICATION OF AWARD

MPCB will notify the successful bidder in writing that his bid has been accepted. Upon the successful bidder’s furnishing of performance security, MPCB will promptly notify each unsuccessful bidder and will discharge their bid security.

9 PAYMENT TERMS

9.1 The Price Bid should be valid for a minimum period of 180 days from the last date of submission of bids

9.2 Following payment terms will be offered to the successful Bidder:

1. Within 15 days of signing the Purchase Order / Work Order Acceptance the Successful bidder will submit to MPCB a PBG for 10% of the value of the order / contract. The PBG shall be in the form of a guarantee of a Nationalised Bank(s) acceptable to the MPCB and shall be valid till 38 months from the date of the Purchase Order / Work Order acceptance.

2. An amount equivalent to 70% of the cost of the equipment value (Item 1, 2, and 3 as per Price Bid in Annexure 4) will be paid on supply of the Integrated IT Security Solution with all the features to MPCB’s satisfaction. This would include all the appliances, devices, software licenses and allied equipment that may be required for completing the installation.

3. Balance 30% of equipment value and 100% of one time installation cost (Item no. 4 as per Price Bid in Annexure 4) will be paid upon successful and incident free operations for 30 days from the date of commissioning (i.e. 30 days from CoOP).

4. Support cost (Item No. 5 as per Price Bid in Annexure 4) will be paid in three equal installments in arrears (i.e. on yearly basis in arrears).

5. All payments will be made after deduction of penalties if any, vide a crossed cheque payable in Mumbai and within 30 days of submission of invoice.

9.3 Liquidity Damages and Penalty:

Out of the total Nine (9) weeks for the project, it is estimated that the delivery of all the equipment will require approximately 5 weeks from the date of LoA. It is expected that the SP should complete the entire installation, configuration, testing, commissioning and handover within Nine (9) weeks from the date of LoA. Non-compliance to these time-frames will attract penalties as follow.
LD: For any delay in delivery of the goods for any reasons beyond Five (5) weeks from the date of LoA, the Board reserves the right to charge LD (Liquidated Damages) at the rate of 1% of the order value for every week of delay or part thereof, subject to a maximum of 5%

of the order value. The Board reserves the right to invoke the PBG in case the delay exceeds 5 weeks.
Penalty: For any delay in installation and commissioning beyond NINE (9) weeks from the date LoA / Purchase Order, the Board reserves the right to charge an LD (Liquidated Damages) at the rate of 2% of the total contract value for the delay of every week or part thereof, subject to a maximum of 10% of the total contract value.

In case the delays in completion of the project exceed FIVE (5) weeks beyond the prescribed Nine (9) weeks, the board reserves the right to get the work executed from any third party at the cost of the successful bidder.

10 INDEMNIFICATION

The bidder hereby agrees and undertakes that, during the Term of the Contract, it shall indemnify and keep indemnified and otherwise save harmless, MPCB from any third party suits instituted against MPCB which are proved to be because of a direct consequence of the installation and / or use of equipment & services provided by the successful bidder.

11 ASSIGNABILITY

The successful bidder will not assign its rights, title or interest in the contract in favour of any third party without prior written consent of MPCB. MPCB reserves its rights to grant such consent on such terms and conditions, as it deems fits and proper. MPCB's decision to grant such consent or refusal to grant such consent shall be final.

12 CONFIDENTIALITY

Successful Bidder shall hold data and information about MPCB, obtained during the execution of its responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of MPCB.

Successful Bidder and MPCB shall maintain in confidence any information relating to the terms and conditions of this contract, information received from each other hereto in connection with this agreement as well as the business operations and affairs of MPCB or the successful bidder and their affiliates and shall not provide access to such information to any third party. This obligation shall expire 2 years after completion of the contract.

13 CORRUPT & FRAUDULENT PRACTICES

MPCB requires that the bidder under this RFP document maintains highest standards of ethics during procurement and execution of this project. In pursuance of this policy the board defines the terms set forth as follows

"corrupt practice" means offering, giving, receiving or soliciting of anything of value to influence the action or decision making of public official in the procurement process or execution of the project.

“fraudulent practice” means misrepresentation of facts in order to influence the action or decision making of public official in the procurement process or execution of the project to the detriment of the board, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the board the benefits of free & open competition.

If it is determined that bidder / s are engaged in corrupt & fraudulent practices their bid/s will be rejected and also will be declared ineligible for indefinite period or a stated period to time to participate in any future RFP floated by MPCB.

14 ARBITRATION

All disputes, differences, claims and demands arising under or pursuant to or touching this document shall be settled by arbitration of sole arbitrator to be appointed by both the parties and failing such agreement, by two arbitrators, one to be appointed by each party to disputes. All arbitrations shall be held at Mumbai location.

15 LEGAL JURISDICTION

All legal disputes are subject to jurisdiction of Mumbai courts only.

16 EXHIBIT 1: FORMAT OF THE COVERING LETTER

***(The covering letter is to be submitted by the* Bidder *along with the Cover 1 of the* Bid)**

Date:
Place:

To,

Member Secretary
Maharashtra Pollution Control Board
Kalpataru Point, 3rd floor,
Opp. Cine Planet Cinema, Sion Circle,
Sion (E), Mumbai – 22

Dear Sir,

Sub: Selection of Solution Provider (SP) for Supply, Installation, Commissioning and Support of Integrated IT Security solution at MPCB

Please find enclosed our Bid for "Selection of Solution Provider (SP) for for Supply, Installation, Commissioning and Support of Integrated IT Security solution at MPCB" in response to the Request for Proposal (RFP) Document issued by **MPCB** dated ………………………..

We hereby confirm the following:

1. The Bid is being submitted by *(name of the* Bidder) who is the Bidder in accordance with the conditions stipulated in the RFP.
2. We have examined in detail and have understood the terms and conditions stipulated in the RFP Document issued by **MPCB** and in any subsequent communication sent by **MPCB.** We agree and undertake to abide by all these terms and conditions. Our Bid is consistent with all the requirements of submission as stated in the RFP or in any of the subsequent communications from **MPCB**.
3. We have paid the EMD as per the RFP terms.
4. The information submitted in our Bid is complete, is strictly as per the requirements as stipulated in the RFP, and is correct to the best of our knowledge and understanding. We would be solely responsible for any errors or omissions in our Bid.
5. We as the Bidder, designate Mr/Ms (mention name, designation, contact address, phone no., fax no., etc.), as our Authorized Representative and Signatory who is authorized to perform all tasks including, but not limited to providing information, responding to enquiries, entering into contractual commitments etc. on behalf of us in respect of the Project.

For and on behalf of:
Signature:
(Authorized Representative and Signatory)
Name & Designation of the Person:

17 EXHIBIT – 2

FORMAT FOR COVERING LETTER SUBMISSION- WITH PRICE BID

(The Price Bid should be submitted along with the following cover letter. Format of Price Bid is given in **Annexure - 4**)

Date:
Place:

To,

Member Secretary
Maharashtra Pollution Control Board
Kalpataru Point, 3rd floor,
Opp. Cine Planet Cinema, Sion Circle,
Sion (E), Mumbai – 400 022

Dear Sir,

Sub: Selection of Solution Provider (SP) for for Supply, Installation, Commissioning and Support of Integrated IT Security solution at MPCB

As a part of the Bid, we hereby make the following price offer to the MPCB.

The cost of the supply, installation, configuration and commissioning of Integrated IT Security Solution appliance Product and support for the same for THREE (3) years is mentioned in the Price Bid as per Annexure – 4 of the RFP.

We agree to bind by this offer if we are selected as the Successful Bidder.

For and on behalf of:

Signature (Authorized Representative and Signatory of the Bidder):

Name of the Person:
Designation:

18 EXHIBIT – 3

MANUFACTURER'S AUTHORISATION FORM AND DECLARATION OF TECHNICAL COMPLIANCE

(This letter of authority must be on the letterhead of the Manufacturer, must be signed by a person competent and having the power of attorney to bind the Producer, and must be included by the Bidder in its bid as specified in the Instructions to Bidders.)

Date:
Place:

To,
Member Secretary
Maharashtra Pollution Control Board
Kalpataru Point, 3rd floor,
Opp. Cine Planet Cinema, Sion Circle,
Sion (E), Mumbai – 400 022

Sub: Selection of Solution Provider (SP) for Supply, Installation, Commissioning and Support of Integrated IT Security solution at MPCB. RFP Ref <RFP reference No.>

Dear Sir,

WHEREAS <Name and address of the Manufacturer> who are official producers of < Name of the product and product code > do hereby authorize <name of the Bidder> located at <Address of the Bidder> (hereinafter, the "Bidder") to submit a bid of the following Products produced by us, for the Supply Requirements associated with the above Invitation for Bids. When resold by Name of the Bidder>, these products are subject to our applicable standard end- user warranty terms.

We assure you that in the event of <Name of the Bidder>, not being able to fulfil its obligation as our Solution Provider in respect of our standard Warranty Terms we would continue to meet our Warranty Terms through alternate arrangements.

We also confirm that <Name of the Bidder> is our authorized Solution Provider / System Integrator and can hence provide maintenance and upgrade support for our products.

We further confirm that

1. We < manufacturer's name> have our product/s <name/s of the product proposed in the bid> listed in the Magic Quadrant for the year 2019 as published by Gartner report / NSS Lab report
2. We have read and understood the technical specifications mentioned in Annexure 2 of this RFP and our product <Name of the product and product code> is 100% compliant to every specification mentioned therein.

We understand that if any of the points in this declaration is found to be incorrect, the bid will be declared as non-responsive and will not be considered for further evaluation.

Name
In the capacity of
Signed
Duly authorized to sign the authorization for and on behalf of : ________________________
Dated :.

19 ANNEXURE – 1

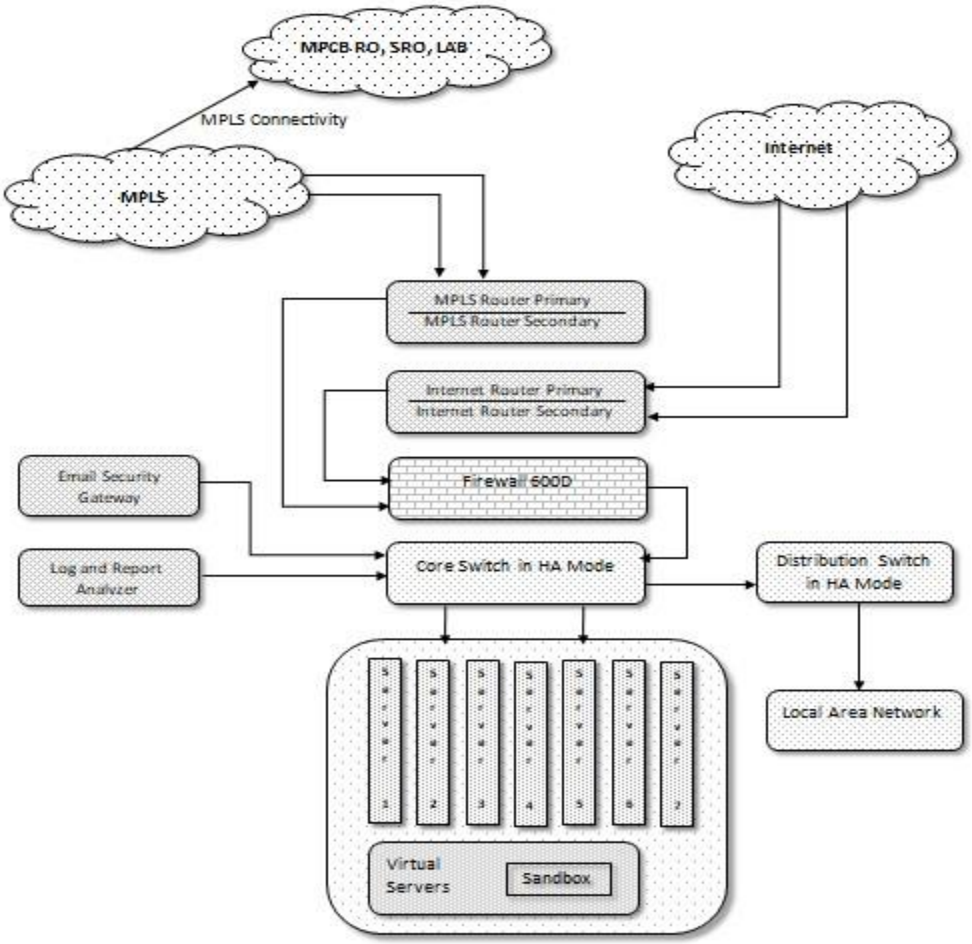
CURRENT INFRASTRUCTURE AND PROPOSED SOLUTION

CURRENT INFRASTRUCTURE

MPCB has an on-site Data Centre facility which has been recently modernized, The modernized infrastructure running on Virtualized Platform is robust, fail-safe and scalable. There are various applications which are accessed by the MPCB users in their regional and sub-regional offices (RO and SRO) and Laboratories across Maharashtra. These offices are connected through MPLS VPN and are protected through a Firewall.

Core Infrastructure Overview

The following diagram illustrates the current IT-Security infrastructure at MPCB. Neither the diagram nor this document touches upon the end-point security which also is an important component of the entire infrastructure.



Key highlights of the current Core Security Infrastructure

- **Firewall:** Currently MPCB have Stand-alone Fortigate 600 D firewall for incoming and outgoing traffic. A Universal Threat Management (UTM) device, this is the fulcrum of the solution. It provides packet filtering, network- and port-address translation (NAT), stateful inspection, and virtual private network (VPN) support.
- **Email Security:** To secure the mail traffic of users, MPCB have fortimail solution which take care of phishing mail, spamming, etc. This solution provides basic message transfer agent functions; inbound filtering of spam, phishing, malicious and marketing emails; and outbound data loss prevention (DLP) and email encryption.
- **Sandbox Solution:** For unknown threats, MPCB has Fortisandbox which is integrated with Fortimail and Fortigate Firewall. The Solution provides an isolated computing environment in which a program or file can be executed without affecting the application in which it runs. MPCB had been a victim of many ransomware attacks in the past and has been effective in avoiding any such attacks since its deployment.
- **Logging and reporting:** To capture the logs and analyse the logs, MPCB have fortianalyzer which is integrated with Fortigate and Fortimail. This sub-system is specifically for having an audit track of the various logs generated by various sub-systems of the solution. This sub-system is an important component for aiding in troubleshooting and post-facto analysis for understanding any possible threat avenues.

All the above equipment is deployed at the Data Centre hosted at MPCB HO. MPCB has also commissioned a Disaster Recovery solution with the DR setup hosted at a facility hosted in Bangaluru.

Application Overview

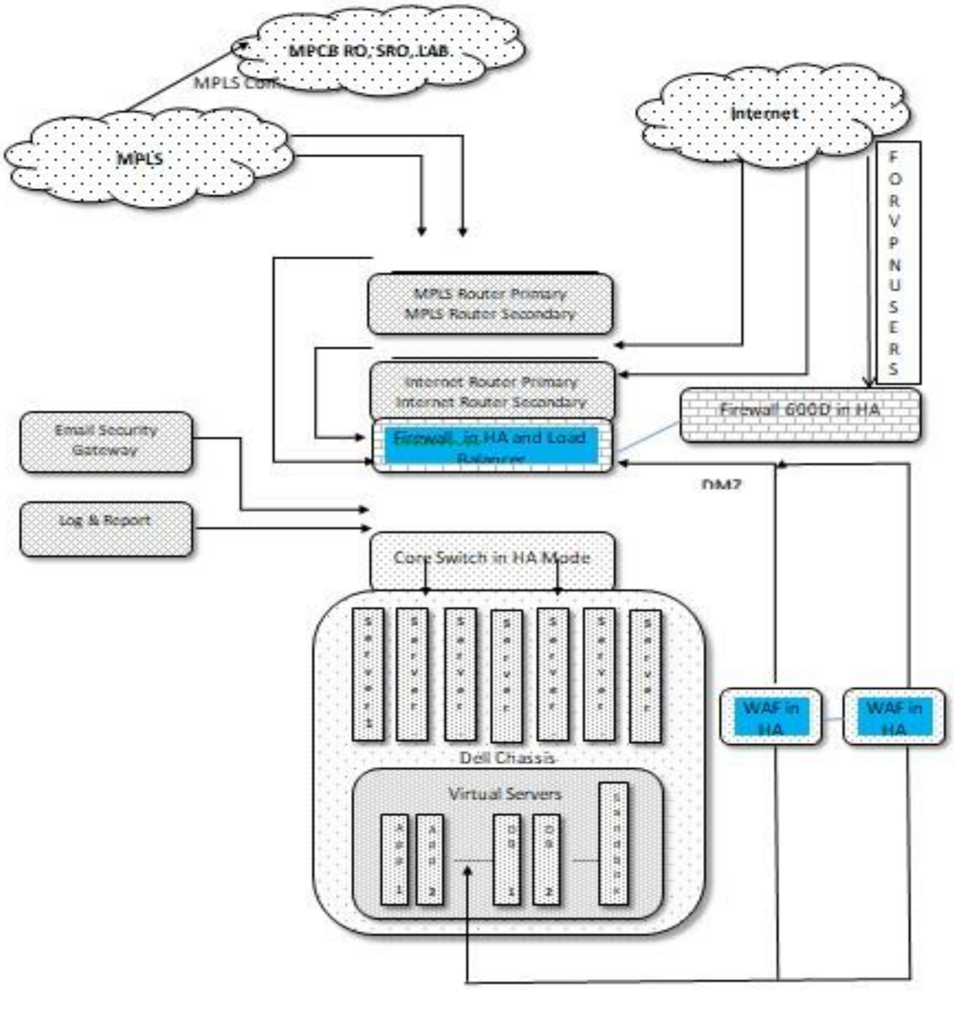
MPCB has been on forefront of embracing the digital initiatives to bring “ease of business” in their citizen charter. In line with the same, MPCB has designed a banquet of bespoke applications, which are hosted in DataCentre at MPCB HO. These applications may pose security risks and hence a brief overview of the respective applications is presented in the table below.

Bidders may at their own costs and with prior appointment of MPCB officials, visit MPCB to understand the current infrastructure. This visit is only to facilitate a better understanding to bidders.

Sr.	Application Name	Approx No. of Users	User Type Internal / External	No of Sessions	Brief Functional Description
1	ECMPCB Application.	Total Users 16,747	External	Approx 3800000 per day	Used by all the industries/health care establishments for applying to all the services provided by MPCB,Upload compulsory attachment,make payment online and download certificate
2	IMIS.		Internal		Used by MPCB Officers for internal proccessing of all the applications,complaints received,create agenda & minutes , file transfer system, generate office notes , initiate legal action against industries , upload inspection report etc. All internal work in MPCB takes place from this portal.
3	SWM Portal.		External & Internal		Used by Municipal Corporations and Council for submission of solid waste generation and collection data on a daily & monthly basis
4	Environment Clearance Portal.		Internal		Used by Environment Department Committees SEAC & SEIAA for processing and disposing of environment clearance certificate
5	Sewage Management Portal.		External & Internal		Used by Municipal Corporations and Council for submission of sewage waste generation and collection data on a daily & monthly basis
6	NACP portal (Non attainment city action plans)		External & Internal		Used by Corportations to update the implementation status of Non Attainment Action Plans on a monthly & quaterly basis.
7	Central Inspection System.		External & Internal		Used by MPCB,Labour Department, DISH & MLWB Department to view inspections allocated and upload inspection report. Used by industries to download their inspection report and submit compliance.
8	Logbook Portal.		External		Used by Industry to submit details of treatment system used in the form of e-logbook on a daily manner.
9	Thermal power plant portal		External		Used by Thermal Power Plants for compliancesubmission of parameter details on monthly, quarterly basis

PROPOSED SOLUTION AND SOLUTION COMPONENTS

The proposed solution is depicted in the schematic below.



Solution Overview

The diagram depicts the proposed solution for MPCB core infrastructure revamp based on the design considerations discussed above and MPCB's current infrastructure and needs.

Key highlights of the solution are as below

1. Two tier architecture, thus a multi-layered security approach: Primary Gateway as first layer of security for authentication purpose and second layer of Web application layer security by application sensitive threat mitigation

2. Redundancy at multiple levels

    a. Primary Gateway : Next Generation Firewall (NGFW) in High availability mode in "Active-active" configuration. It also acts as load balancer. Ensures uncompromised functionality even if one of the appliance box fails / is unavailable

    b. Web Application Firewall : Deployed in High-availability mode. It should support Active/Standby, Active/Active and N+1 modes.

3. Introduction of Security Infrastructure and Event Management (SIEM)

4. Re-use of existing infrastructure components such as Email security, Sandbox and Logging and Reporting

5. Re-deployment of existing Firewall for a new gateway which can be used for VPN connectivity of remote users.

6. Internal segmentation of Network by forming VLANs

7. No single point of failure and secure remote access in case of remote users

Building blocks of the solution

The entire solution is an integration of various building blocks. These building blocks are also sub-systems which are purpose built to have their independent role and functionality as a part of the overall solution.

I. Next generation Firewall (NGFW)

i. Next generation firewall with High availability and will be placed at Internet gateway level.

ii. NGFW will take care of IPS, Gateway Anti-virus, Web-filtering/Contain Filtering, Application control, Anti-Spyware, Anti-Botnet, internal segmentation, Known attack and zero day attack including Memory based and preventing Side Channel attacks.

iii. NGFW can also act as Secure WAN for future requirement, with features like WAN & Application load balancing from day one.

iv. NGFW will be integrated with existing sand-box for zero-day attack prevention and/or should have separate in premise integrated sand-box solution with proposed NGFW.

v. NGFW will also help MPCB for TLS 1.3 deep inspection. The proposed solution should have inbuilt features to integrate with LDAP (multiple domains), XAUTH/RADIUS, SSO Server from day one.

vi. NGFW will prevent from DOS attack

II. Web Application Firewall (WAF)

i. Web Application Firewall will protect the applications reside in DMZ.

ii. It is proposed to have the WAF in a redundant High Availability mode. It must be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode. In addition it should also perform as reverse proxy and forward proxy

iii. Web Application Firewall should stop advance application layer attack, behavioural DOS attack, application layer (L7) D-DOS attack.

iv. Multi-core processor technology combined with hardware-based SSL tools deliver blazing fast protected WAF throughput

v. Protection from the OWASP Top Ten application attacks including Cross Site Scripting and SQL Injection. In addition it should support proactive bot defence specific to mobile apps through use of mobile SDK

vi. Dual-layer machine learning engines are employed to detect application request anomalies and determine if they are threats.

vii. Web Application Firewall will take care of following attack

- IP reputation
- Behavioural Ddos attack across all virtual servers using advanced analytics and ML to generate dynamic signatures and block malicious traffic without administrator intervention.
- Protocol validation
- Known application attack
- Virus, malware, loss of Data.
- zero day attack protection
- Credential Stuffing and application layer encryption services
- Machine learning capability to detect and block unknown attack.

III. Internal Segmentation – purpose built and application sensitive

i. Internal segmentation will help MPCB to segregate the user traffic and application server traffic.

ii. Only authorized traffic will be allowed to access the application server of database.

iii. While accessing the applications-server, that user will be inspected by firewall, so that this will stop threats lateral movement.

IV. Security Infrastructure and Event Management (SIEM)

i. SIEM can be a software based solution and will help MPCB for logs correlation between different security vendors.

ii. SIEM will automate the incident response to mitigate the threats.

iii. SIEM will help MPCB for cross correlation between network devices (NOC) and Security devices (SOC).

iv. SIEM will help for single plan visibility of threats in entire network.

V. Email Solution

Existing Fortimail solution should be re-used as this is sufficient to address the following types of attacks

1. Phishing Attack.
2. Virus Attack
3. Spamming and Spoofing
4. Zero Day attack (through integration with Sand-box)
5. DLP
6. DMARC,SPF & DKIM
7. Encryption

VI. SandBox

i. MPCB is already using FortiSandbox. Fortisandbox is used to identify the advanced threat and zero day attack. The Solution provides an isolated computing environment in which a program or file can be executed without affecting the application in which it runs. MPCB had been a victim of many ransomware attacks in the past and has been effective in avoiding any such attacks since its deployment.

ii. The existing sandbox solution can be integrated seamlessly with the proposed solution.

iii. Following are the features of Fortisandbox

1. AI-powered Sandbox Malware Analysis.
2. Mitre ATT&CK-based Reporting and Investigative Tools
3. Automated Breach Protection

VII. Redeployment of Existing Firewall (Fortigate 600D)

In the near future, working from homes and / or working from field are going to be a norm rather than an exception. For example, field officers may require to log in to

IMIS or any other relevant application from the field over WAN. In such situations, it is a MUST that the established connective is secure and the respective user is authenticated. Thus this is going to be a requirement of the MPCB IT infrastructure.

In order to specifically segregate such individual users wanting to access MPCB network need proper authentication. Considering this MPCB wishes to redeploy its existing Fortigate 600D will be used for SSL VPN traffic.

Location for deployment of proposed solution:

The Integrated IT Security Solution should be deployed, configured and commissioned at the infrastructure available at the Data Center at following location.

Sr. No.	Office	Location
1	Head Office	Maharashtra Pollution Control Board Kalpataru Point, 4th floor, Opp. Cine Planet Cinema, Sion Circle Sion (E), MUMBAI – 22

20 ANNEXURE – 2

TECHNICAL COMPLIANCE

(This format must be filled completely clearly indicating the feature-wise compliances and deviations, if any, with respect to the product proposed to be supplied. The form needs to be printed on the letterhead of the Manufacturer / OEM, must be signed by a person competent and having the power of attorney to bind the Producer, and must be included by the Bidder in its bid.)

A. COMPLIANCE / DEVIATION FOR NEXT GENRATION FIREWALL (QTY: 2) (to be deployed in High availability mode)

Name of the Product Proposed : ______________________________

Product Code (if any) : ______________________________

Sr. No.	Feature Description	Compliance (Y/N)	Deviation
A.	**General Specifications**		
1	The proposed NGFW should be a dedicated appliance-based solution.		
2	Should have built-in storage of at least 1 TB, 1 console Port , 1 USB interface and dedicated management Port		
3	Should support REST APIs for management		
4	Threat prevention/NGFW/UTM throughput of 6 Gbps or higher. The Firewall should have at least 3 Gbps of IPS throughput or higher. VPN throughput at least 3 Gbps or higher. The Firewall should support at least 40,000 new sessions/connections per second. Inbuilt DUAL redundant Power supply and removable fans installed and available The Firewall should support at least 4 million maximum connections and 35K maximum DPI SSL sessions/connections. Should support at least 6,000 IPSec Site-to-Site VPN tunnels and 6000 or more no of IPSec Client Remote access VPN Should support at least 1500 SSL VPN users Solution should support IPSEC & SSL VPN and Layer 2 Tunnelling protocol (L2TP)over IPSEC Should have minimum of 20 x 1GbE interfaces, 4 x 1Gb SFP interfaces, 2 x 10Gig Ethernet (Cu) interfaces and 2 x 10Gig SFP+ interfaces		
5	Appliance should support Active/Passive with State Sync, Active/Active Clustering. Configured with Active-Active configuration from day 1.		
B.	**Security Features**		
1	Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware, Application Control and Geo-IP protection. The firewall should also support anti-Spam services.		
2	The device should be IPv6 ready (Both phase 1 and Phase2), and should support multi-core architecture and should have IPv6 and should support filtering and wire mode implementations.		
3	Appliance should support IPSec NAT traversal, OSPF, RIP V1 & V2 routing protocol and NAT without degrading performance of the firewall.		
4	Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix		
5	Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode		

7	Should be quad core or higher processor-based solution for faster processing. The firewall should support at least 10 Security Processing Cores. The processor should not be proprietary ASIC based.		
8	Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol.		
9	Should proactively detect and block mass market, zero-day threats and unknown malware by inspecting directly in memory		
10	Should have capability to look deep inside every packet (the header and data) searching for protocol non-compliance, threats, zerodays, intrusions, and even defined criteria. The firewall should support stream/flow-based inspection only without compromising/missing any security features like AV, Windows File Sharing (CIFS), email filter, web filter, VOIP etc.		
11	Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration		
12	Should allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.		
13	Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.		
14	Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.		
15	Should have H.323 gatekeeper and SIP proxy support to block spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.		
16	The proposed solution should be scalable and offer fault tolerance to safeguard against hardware failures. The failover should be capable of taking over the traffic without any manual intervention and session loss.		
17	Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found. And should not buffer traffic before scanning for virus.		
18	Should have TLS/SSL decryption and inspection engine that decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic.		
19	Should have deep packet inspection of SSH to decrypt and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.		
20	Should support REST APIs that allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.		

21	Should have Bi-directional raw TCP inspection. The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.		
22	Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decode payloads for malware inspection, even if they do not run on standard, well-known ports.		
23	Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1.		
24	Should control applications, or individual application features, that are identified by the security engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity. Should control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.		
25	Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. Appliance should protect against DOS & DDOS attacks .		
26	Should have anti-evasion technology by using extensive stream normalization, decoding & other techniques ensuring threats do not enter network undetected by utilizing evasion techniques in Layer 2-7		
27	Should not buffer traffic before scanning for IPS and must support inbound and outbound IPS scanning. It should scan the entire traffic and not few specific kilobyte of the session.		
28	Should be integrated solution with appliance based firewall on a single chasis with multicore processor.		
29	The device should be featured with Gateway Antivirus and DPI SSl Scanning and should support minimum 20000 DPI/IPS signature		
30	Should be an unlimited user-based appliance. Firewall must support inbound and outbound Antimalware/Antispyware scanning. Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.		
31	Should enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.		
32	Should block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.		
33	The firewall should be integrated with sandboxing solution from the same OEM which should be appliance based and deploy sandboxing engine for effective scanning.		

34	Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. Technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen.		
35	Firewall should have capability to block/prevent from Side Channel attack like Meltdown, Spectre,Foreshadow, Foreshadow-NG, Portsmash etc. Should have support for file send to proposed on premise Sandbox for analysis to be held at the gateway until the verdict is determined		
36	The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol.		
C	**Logging and reporting**		
1	Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.		
2	Should be integrated with third party SIEM		
3	The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.		
4	The solution should help to analyze/understand the live application usage in the network.		
5	Solution should run its own syslog server or integrated server to collect the logs. If separate server and/or appliance is required for the logging & reporting , the BOM & cost should be included in the proposed solution.		
6	The solution should provide Change Order Management and Work Flow which assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment.		
D	**Licensing and Support**		
1	The devices should not have license restriction on number of users. The license should have the following subscriptions from day 1 - Firewall, Gateway Anti-Virus, AntiSpyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and Advance Threat Prevention/Protection including advance sandboxing.		
2	The OEM should have Common Criteria/NDPP and ICSA Enterprise Firewall certification.		
3	Entire NGFW and sandboxing solution of software and subscription shall be from dedicated appliance based by same OEM and should support integration with SIEM solution		
4	Solution should have 24*7 Support and Advance hardware replacement by OEM		
5	All license should be perpetual and with 3 Years cover for update and upgrade (Include Minor , Major update in software and firmware)		
6	Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation along with 3 years security software subscription.		

B. COMPLIANCE / DEVIATION FOR WEB APPLICATION FIREWALL (QTY: 2) (to be deployed in High availability mode)

Name of the Product Proposed : ________________________________

Product Code (if any) : ________________________________

Sr. No.	Feature description	Compliance (Y/N)	Deviation
1	The proposed WAF should be a dedicated appliance based solution.		
2	WAF should support minimum Performance parameters as below: a. 600k L4 HTTP Request Per Second. b. 2.5K SSL TPS with RSA (2K Key) and 2.1K with ECC. c. 5 Gbps of SSL Throughput d. L4/L7 Throughput 10Gbps. e. Appliance should max 16 GB RAM DDR4 & 500 GB HDD. f. 4x 1G SFP & 2 x 10 GbE SFP+ SR.		
3	Solution should include a LCD panel which should support Configuration for Initial Management IP address and display all the error and information corresponding to hardware & software without logging into the appliance.		
4	Appliance should be able to perform in multiple modes such as Active, passive, Transparent, proxy mode etc.. Should perform as reverse proxy and forward proxy. Deployment should be in High Availiblity mode		
5	Must support OWASP Top 10 attacks, Anti-Bot Mobile DDoS protection and application layer encryption, Parameters Tampering, Cookie Poisoning, SQL Injection, protect cookie poisoning and cookie tampering, protect certain hidden form fields, Cookie Poisoning and must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.		

6	The solution must provide the following features and protection: - HTTP protocol validation - Correlated based attack protection - HTTP protocol attack signatures - Cookie signing validation - Anti site scraping - Bot mitigation - Whitelisting based protection - Web worm protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation - Proactive bot Defense with ability to detect if the Bots are using Captcha farms to bypass the Captcha challenge. - Sensitive data exposure - Behavioral & Stress based detection - Heavy URL protection - Sloris attacks - Web Page parameter Security - forceful Browsing - Cookie Tampering		
7	The WAF must be able to auto detection and mitigation of L7 DoS attacks using machine learning		
8	The WAF must have application-ready security templates for applications. Eg. Microsoft Sharepoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino for rapid deployment		
9	The WAF must be extensible with add-on license to provide API Authentication, and support oAuth 2.0.		
10	WAF should support for IPv4 and IPv6 traffic. It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)		
11	WAF should support inbuilt capability to protect against the mobile/tablet, application-based attacks through Anti-Bot Mobile SDK which whitelist establish trust based on an embedded software package within the application code and corresponding cookie verification to protect application against attacks generated from mobile.		
12	Policies must be automatically generated from auto learn results, Auto-learn options should be available to tweak and fine tune rules. The auto learn policy should have provision to put into staging mode for specific time period to avoid the false positive.		
13	The WAF should be able to allow or deny traffic based on IP address. It also should be able to protect FTP and SMTP traffic by allowing only legitimate commands and doing protocol sanitation checks.		
14	Must provide inbuilt capability to encrypt the user credentials in real time. Users typing the credentials on web browser for any web application should be encrypted in real time to protect against browser-based malware. This feature should be agentless and should not require installation of any kind of software either on client or application side.		

15	WAF solution should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration with third party AV and DLP solution. It should also support thrid party integration with commercials and opensouce with threat intelligence e.g. HTTP connector.		
16	The WAF solution should have inbuild HTTP to MQTT Parser. Solution should provide certificate based authentication between IOT devices.		
17	The proposed appliance must be able to load balance both TCP and UDP based application from L2 to L7 including lightweight MQTT protocol for machine to machine connectivity between IoT appliances such as small sensors, mobile devices etc.		
18	API authentication and API Gateway protection, Protection against SYN-flood type of attacks, Buffer Overflow Attacks, It should have controls against Brute force attacks, Cross-Site Scripting (XSS), Brute Force Attacks, Custom brute force attack detection for applications that do not return 401, Cross Site Request Forgery (CSRF),		
19	WAF should have predictable performance and reduced latency and should run as dedicated service on the proposed appliance. Must leverage hardware based acceleration architecture with FPGA’s/ASICS technologies.		
20	WAF must support API authentication and API Gateway protection and should have application layer encryption using HTML field obfuscation against malware based attacks.		
21	The solution should support protection from password cracking behavior by analyzing login credentials, identifying login field, browser fingerprint and IP address.		
22	Must provide ability to allow or deny a specific URL access and must have ability to define different policies for different applications & must have ability to create attack signatures or events and should support to prevent of theft and mitigation of attacks that uses previously stolen credentials.		
23	WAF should support application layer Password Encryption to protect against Browser based Malware. It should be able to encrypt the user credentials in real time so as to protect any sensitive parameter as defined by department to protect from keyloggers and credential stealing malware residing in the end users system.		
24	The proposed WAF should support the following Security Features/Functionalities: a. Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1, HTTP 2.0 client side and server side both. b. Should validate header length, content length, Body length, Parameter length, body line length etc..		
25	The client certificates should be supported in passive mode and active mode. In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL, XML Security Protection and XML encryption feature.		

26	The solution should have capability to protect Credential Attacks Protects against attacks that can steal credentials from the user's browser.		
27	The WAF should support inbuild credential stuffing database to protect against compromised credentials.		
28	WAF should support inbuilt PCI DSS compliance. In addition the solution must support integration with third party DAST tool to perform virtual patching for its protected web applications.The solution must support proposed web application vulnerability assessment tolls to virtually patch web application vulnerabilities.		
29	The proposed WAF should be able to authenticate users based on browser type and version, operating system type and version.		
30	WAF should support client certificate constrained delegation (C3D) which will enable the Load balancing solution to generate certificates on behalf of clients and pass it to the end servers if SSL based client authentication has been enabled on the backend servers .		
31	WAF should provide the application visibility and reporting metrics and entity for each application like Client IP addresses / subnets as well as geographical regions, Total Transactions as well as Average and Max Transactions/sec, Most commonly requested URLs, Virtual Server and Pool server performance, Page Load Time, Response code, OS and Browser, URL details, Server Latency and Page Load times		
32	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must be continuously and automatically updated.		
33	The solution must provide the ability to comply to A+ Certification at the click of a button.		
34	Offered solution should be EAL4+ or NDPP (Network Device Protection Profile) certified under Common Criteria Program for security related functions.		
	License and Support		
1	Entire WAF solution of software and subscription shall be from same OEM and should be integrated with SIEM solution		
2	Solution should have 24*7 L3 Support and Advance hardware replacement by OEM		
3	All license should be perpetual and with 3 Years cover for update and upgrade (Include Minor , Major update in software and firmware)		
4	Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation along with 3 years security software subscription.		

C. COMPLIANCE / DEVIATION FOR SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Name of the Product Proposed : ______________________________

Product Code (if any) : ______________________________

Sr. No.	Feature Description	Compliance (Y/N)	Deviation
A	**General**		
	Automated Log Collection: The proposed solution must provide agent-less solution that can automatically scan the list of devices (servers, switches and other devices) to be monitored and will automatically accept events and automatically start monitoring devices without any administrator intervention.		
	Automated Log Management: The proposed solution must provide a log management solution that would require very little post-deployment effort for tasks such as introducing new event sources, managing retention policies and archiving of log data. It must retain both RAW and Normalized logs for one year. Log management layer must provide High availability.		
	Automated Analysis: The proposed solution must provide the ability to start analyzing and correlating activity out-of-the-box. The product must assist security analysts by reducing false-positives automatically without configuring any rules or filters to do so.		
	Workflow Automation: The proposed solution must provide a SIEM solution that can initiate workflow that will automatically open tickets, assign the tickets to the appropriate team members while maintaining a complete audit trail for the incident handling process.		
	Deployment Methodology:		
	Solution must be software based which should be capable of running on Virtual machine. Bidder is required to provide sizing sheet for all hardware such as servers, storage, OS etc. required to run the system. Collection / receiver should be software based and must be free for unlimited remote sites for future expansion and should be compatible with all types of hardware / OS platform. Collection / Receiver should also support load balancing out of the box. At least, load balancing should support syslog event devices and Windows event logging.		
B	**Event Collection**		
	Device Support: The proposed solution must provide a comprehensive out of the box coverage across all types of event sources not limited to Databases (SQL Server 2005, 2008, 2012, Oracle), AIX Servers, Unix/Linux Servers, Windows Servers, Routers, Switches, Gateways, hubs, Windows OS 8, 8.1, 10, firewalls, UPS, for all types of OEM products.		
	Out of the box Custom Web Application Support: The proposed solution must provide a native, out of the box capability to collect application log data from custom /in-house developed web applications, without explicit custom parser development.		

	Application Support The proposed solution should be capable of collecting events from SAP applications for audit, access and security logs (SQL injection, XSS or any kind of security vulnerability).		
	Retrofit Logging Capability: The proposed solution must retrofit with any application, which may or may not generate logs. It should be capable of collecting events from all Applications.		
	Distributed Event Processing: The proposed solution must collect logs in a distributed manner, offloading the processing requirements of the log management system for tasks such as filtering, aggregation, compression and encryption.		
	Custom Collection API: The proposed solution must have a software tool to allow customers to create integration with unsupported legacy or internally developed event sources. The software tool must allow customers to integrate with Syslog, log files and databases and support the ability to parse multi-line log files.		
	Normalized Event Data: The proposed solution must normalize all collected event data into a consistent format suggested by NIST 800-92(National Institute of Science and Technology).		
	Collection Health Monitoring: Any failures of the event collection infrastructure must be detected immediately and operations personnel must be notified. Health monitoring must include the ability to validate that original event sources are still sending events.		
	Event Filtering: The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed.		
	Event Prioritization: The proposed solution must provide transaction assurance whereby high priority log events can be prioritized and immediately analysed.		
	Event Aggregation: Aggregation must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows. An example of aggregation would be every 1000 identical events be aggregated into one record with the necessary start and end timestamps and the aggregate count of 1000. Aggregation must provide up to 25% event reduction before any data is processed by the system.		
	Compression: The proposed solution must provide at least 70 % compression which can be customized for the data to provide further bandwidth conservation.		
	Raw Event Data: proposed solution must support the option of collecting raw event data using Syslog, FTP, SCP, SNMP, checkpoint firewall protocol, and any other protocol required for collection of logs etc. This ensures original audit quality data is available for forensics.		
	Centralized Management: The proposed solution must be managed centrally allowing users to configure all features, backup configurations and push software updates etc. using one centralized interface.		
	Event Replay: The proposed solution must provide a software based tool or facility which allows production event data to be exported and replayed into the system for testing and content creation.		

	No Events are Dropped during Spikes, even If the License has been exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.		
	Log Management - Analysis and Search		
	Retention Policies: The proposed solution must provide the ability to create multiple policies for the automated retention and disposal of log data.		
	Search Interface: The proposed solution must provide a simple, intuitive search interface usable by different users with varying skill sets.		
	Search Drilldown: The proposed solution search interface must provide the ability to drilldown on output data and alter the search filter by simply click on fields within an event.		
	Flow-based Searches: The proposed solution must allow easy and intuitive query structures which allow to compound search expressions into complex patterns, similar to what would otherwise require "piping" multiple commands into scripts using traditional tools, without requiring any knowledge of scripting languages.		
	Search Method Combination: The proposed solution search interface must provide the option to allow combined search queries using a combination of methods such as indexed and non-indexed event data and regular expression and full unstructured text search simultaneously without impacting search performance.		
	Log Management – Security		
	Log Data Integrity: Proposed solution must provide integrity mechanisms in accordance with NIST 800-92 such as digitally signing data with a secure hashing algorithm so that logs cannot be altered or deleted.		
	Granular Access Control: The proposed solution must provide role-based access control with granular access to all components and features.		
	Logical Data Segregation: The proposed solution must provide logical segregation of log data that can be viewed by different teams. Various operating teams can only see "their" device event data which provides separation of duties.		
	Centralized Authentication: The proposed solution must support integration with a central account management system i.e. Active Directory.		
	Log Management –Administration		
	Administration Dashboard: The proposed solution must provide a single administrative dashboard used only by administrators to analyse the system load, event flow and storage performance trends.		
	Device Discovery: Proposed solution must automatically accept log data from any system that is reporting through system. All log data, once received and indexed should be available for searches, alerts, and reports.		
	Administration Audit Trail: The proposed solution must log all administrative access and activities and provide access to the audit logs through the same web interface.		

	Centralized Configuration Management: The configuration of proposed solution must be centralized managed to reduce operational overhead of the solution and ensures the consistency of the changes. The central management's audit logging must be able to be stored within the Log Management's secured event data store and/or to be forwarded to SIEM system for real-time monitoring.		
	Log Management – Alerting		
	Real-Time Alerts: The proposed solution must be capable of generating alerts based on filter pattern matches for operational health monitoring.		
	Threshold Alerts: In addition to real-time alerts, the system must provide historical, threshold alerts, configured from saved search queries.		
	Alert Filters: The proposed solution must provide pre-defined alerts and provide the ability to re-use pre-defined filters and own created filters as alert criteria.		
	Alert Delivery: The proposed solution must provide options of how alerts are delivered to operations or security personnel. At a minimum the options must include reporting to the web console, send an email or generate an SNMP trap to an external management system. The solution must be capable of doing all three concurrently for each alert.		
	Lookup Correlation: The proposed solution must provide static correlation based on lookup files (watch list)		
	Log Management – Dashboards		
	Customizable Dashboards: The proposed solution should provide dashboards specific to each user and should be user configurable. The dashboards must be capable of displaying multiple daily reports specific to each users job function.		
	Dashboard Integration: The proposed solution must be accessed through outside systems so that display dashboards, queries and reports can be executed and viewed. Solution should be present on external “Intranet” applications leveraging SOAP calls through WDSL, Apache-Axis and Command Line interface.		
	Log Management – Integration		
	Alerting: The proposed solution should provide the ability to integrate with enterprise-class network management systems through SNMP.		
	Security: The proposed solution should provide the ability of bidirectional integration with enterprise systems to provide a complete security operations ecosystem (real-time correlation, threat response, alerting, annotation, ticketing, compliance reporting). The Solution should allow easy and seamless integration with external enterprise systems.		
	Syslog Forwarding: The proposed solution must be able to receive raw (i.e. unprocessed) event data in the form of syslog messages or text log files, in addition to receive the raw original event data from collectors.		
	Correlation - Analysis and Workflow		
	Correlation Rules: The proposed solution must provide many correlation rules out-of-the-box to automate the incident detection and workflow process.		
	Cross-Device Correlation: The proposed solution must be capable of correlating activity across multiple devices out-of-the-box to detect authentication failures, perimeter security, worm outbreaks and operational events in real-time without the need to specify particular device types.		

	Geo-Spatial Location Correlation: The proposed solution must provide the ability to monitor activity between multiple geographical locations and calculate distances, identify countries of concern and be able to provide country information and GPS coordinates for every event.		
	Dynamic / Static Lists: The proposed solution must allow users to define either whitelist or blacklists that can be used as inclusion or exemption during the correlation process. Additionally, the correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, session tracking, attack history and privileged system access. Product must support import capability to create/ update monitoring list which can be dynamically add/ remove values without manual intervention.		
	Correlation Performance: The proposed solution must be capable of efficiently presenting categorized data to the correlation engine to allow real-time detection and response.		
	Rule Chains: The system must provide the ability to allow rules to be triggered in a series, matching various correlation activity before an alert is generated.		
	Real-time Prioritization: The proposed solution must be capable of assessing attack vectors and the targeted systems to determine the susceptibility of a threat and lower the priority if the target is not susceptible and raise the severity if the target is susceptible or the user is not authorized to access the target system it also have business intelligence and asset intelligence		
	Incident Tracking: The proposed solution must provide necessary tools to identify, isolate and remediate incidents as they occur.		
	Integration Command: The proposed solution must provide integration commands that can execute a local or remote script for tools to assist administrators and/or analysts. Tools such as nslookup, ping, traceroute, portinfo, websearch and whois should be available and preconfigured in the console to access on the local machine.		
	Personalized Threat Intelligence Integration: The proposed solution must provide a built-in out-of-box capability where the users can personalize the trigger/threshold scores against DNS and/or IP addresses in each category for security risk tolerance.		
	Detection and Prevention of Data Exfiltration: The proposed solution must provide out-of-the-box real-time detection and inform if any communications occurs with known malicious hosts such as botnet and/or other hosts on the Internet known to host/facilitate data exfiltration by malwares.		
	Monitor and Protect the Enterprise's Reputation: The proposed solution must provide out-of-the-box capability to monitor internal assets against the reputation database, and most importantly the ability to request removal of internal assets from the reputation database and its upstream data providers once the threat has been eradicated/remediated.		
	Correlation - Reporting and Visualization		

	Future Proofing: The proposed solution must provide a level of confidence that reporting will continue to work and not have to be modified if a particular technology, such as a Firewall or IDS product, is replaced with a newer product or OEM. The reports should continue to run and include the new technology into the report criteria automatically , should have Ad hoc Report Performance with Custom Dashboard and Dashboard Drill-Down:		
	Logical Diagrams: The proposed solution must provide the ability to import graphics from applications such as Visio and overlay chart objects to provide logical visualization of the enterprise network architecture, business processes or application specific components. This function will provide a visual mapping of alerts to enterprise specific components.		
	Attack Visualization: The proposed solution must provide the ability to visually represent event data into a dynamically updated graph. This will assist analysts in determining the expanse of attacks and pinpoint the original attacker during incident response and remediation.		
	Correlation - Advanced Use Cases		
	Compliance Automation: The proposed solution must provide value in assisting in adhering to audit requirements, alerting of non-compliance and providing necessary reports that can be used during an audit.		
	Business Process Monitoring: The proposed solution must provide the ability to monitor and visually display statistics for all dependent components used by business applications from start to end of a transaction. This includes the ability to monitor latency between components, excessive resource usage, errors during process flow and other business logic required to troubleshoot business applications.		
	Zero-Day Threat Intelligence: The proposed solution must provide automatic detection of a 0-day worm outbreak across the enterprise when IDS or Antivirus signatures are unable to detect the incident. The system must then immediately send alerts and automatically start the incident triage and workflow.		
	Forensic Investigations: The proposed solution must be capable of allowing investigators to restore a year's worth of historical log files to a single appliance and then perform complex pattern searches and reporting against terabytes of data in a short period of time.		
	Business Insight to Security Intelligence: The proposed solution must be able to map IT Assets to Business Functions, and report on the Business Risk in the form of heat maps, reports, and scores against Key Performance Index (KPI).		
	Application Analytics : The proposed solution must be capable of collecting logs (Both security and audit) from applications even if application is not generating logs natively and give complete view of attacks, vulnerabilities in applications.		
F	**Security Orchestration and Automation Response**		
	The SIEM solution should have SOAR solution bundled and integrated with it to provide industry best Security Orchestration and Automation Response capabilities that form the part of next generation SOC or SOC 2.0		
	SOAR solution should be fully programmable and adaptable for Security Operations thereby allowing to define workflows and playbooks		

	SOAR solution should have automated Alert Triage and Consolidation features and capabilities		
	SOAR solution should have automated Alert Investigation and Response features and capabilities		
G	**Data Privacy**		
	The solution should have capability to provide field level format preserving encryption to protect PII/PHI from logs at log collection tier.		
	The solution should support stateless key architecture so that it will not induce key management overhead.		
	The proposed solution should work without schema changes in the databases where private data may reside.		
H	**Licensing and Certification**		
	The SIEM License should support deployment in HA or DR or create multiple instance of software license without any additional cost		
	The solution should be able to handle at least 2500 sustainable eps and 10,000 peak eps burst on same infrastructure without any limitation on log sources, flows and people managing the system.		
	Entire solution should be for 36 months.		
	Solution should have 24*7 Support by OEM		
	All license should be perpetual and with 3 Years cover for update and upgrade (Include Minor , Major update in software and firmware)		
	Vendor & OEM should support the appliance / software with all necessary upgrade for at least 3 years from the date of purchase installation along with 3 years security software subscription.		

21 ANNEXURE – 3

SCOPE OF WORK

1.0 SCOPE OF WORK

The successful bidder will take total responsibility for providing and seamless commissioning the Integrated IT Security Solution into MPCB network, as per the given configuration.

The scope of work includes:

A. ONE TIME ACIVITY

1. Study and understand the current IT security infrastructure deployed at MPCB.

2. Prepare a plan for implementation and commissioning of the revamped solution. The proposed plan should mention all dependencies and should ask for minimum downtime, preferably during non-working / non-peak hours for MPCB. The plan should provide for sufficient contingencies and roll-back period, if required.

3. Supply of all the components of the Integrated IT Security Solution i.e. appliances, software, etc. with provision of version upgrades/patches.

4. Study / Create IT Security policies as per MPCB's security architecture design & pattern of traffic; this will include device rules / device policy definition and enforcement on the boxes proposed in this RFP.

5. Installation and configuration of all the components to comply with the proposed solution, so that they seamlessly integrate with existing infrastructure. Major component / subsystems are

   - Next Generation Firewall in High Availability mode with all features
   - Network segmentation as required by MPCB
   - Web Application Firewall in High Availability mode with all features and policies for different applications
   - Sandbox solution integration
   - Email security solution integration
   - SIEM installation, configuration to integrate with all relevant subsystems to give reports and analysis as required by MPCB
   - Re-deployment of current firewall as depicted in proposed solution

6. Solutions should be configured to prevent Zero-day attacks

7. Solutions should be configured isolated computing environment in which a program or file can be executed without affecting the application in which it runs

8. Installation of the proposed appliance will include migration of policies and configuration of the existing firewall.

9. Performance tuning- Performance tuning such that the solution operates as proposed on the production network.
10. Rule/signature tuning- Maximizing the number of rules which can be run in full blocking mode. Preferred plan is to run all rules in monitor mode at first and turn on blocking over time to minimize downtime and risk to our production environment.
11. Provision of all licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
12. Successful bidder should train the identified MPCB officials on the product which includes Central Console Management, log analysis, configuration etc.
13. Preparation of comprehensive documentation depicting appliance, software configuration along with Rules and Policies

B. ON GOING ACTIVITY

1. Comprehensive onsite warranty of 3 year for all the hardware / software under the project. The licenses should be perpetual and should include 24x7 level 3 support for three years with free patches and version upgrades for the period.

2. Review policies periodically and make necessary changes to accommodate prevention of new threats.

3. Monitor implementation of appliance, rules, signature, etc updates periodically.

4. Proactively inform MPCB about forthcoming threats and precautions to be taken.

5. Performance / Rules tuning as and when required to tune the solution operates as proposed and improved performance on the production network

6. Update documentation as and when any change is made in configuration, rules or policies.

MPCB Responsibility

1. Facilitate access and information (IP schema, Network details, etc.) availability to the Project Management Consultant (PMC) and the Solution Provider (SP)
2. Acceptance of the Implementation schedule provided by SP after due review with MPCB / PMC.
3. Ensuring availability of the downtime based on the implementation schedule on reasonable notice given by the SP after consultation with PMC.
4. Ensuring data backup for the servers and storage.
5. Ensuring support availability from the respective Vendors for the Hardware, Networking, UPS, ISP, Application Software whenever required during revamp.

6. Ensuring availability of various vendors such as MPLS Service Providers, Application development partners, current Service Providers, FMS service providers and any other agency – internal and / or external, as may be required.
7. Issue of CoOP upon receipt of satisfactory project implementation and documentation.

22 ANNEXURE – 4

PRICE BID FORMAT

Note: ***Commercial Offer has to be entered online only. An Online Form, similar to the Commercial format given below, will be available to the bidders in Commercial Envelope (C1) during Online Bid Preparation stage where bidders would quote their offer.***

The bidders should strictly follow the format given below for submitting the price –bids

Sr. No.	Description	Qty (Q)	Basic Price (Rs.) A	Taxes (Rs.) B	Total Price (Rs.) T = Q *(A+B)
1	Supply of Next Generation Firewall as per specifications and licensing requirements mentioned in Annexure-2 with THREE (3) years 24 x 7 On-site warranty support	2			
2	Supply of Web Application Firewall as per specifications and licensing requirements mentioned in Annexure-2 with THREE (3) years 24 x 7 On-sitewarranty support	2			
3	Supply of Security Infrastructure and Event Management (SIEM) as per specifications and licensing requirements mentioned in Annexure-2 with THREE (3) years 24 x 7 On-site warranty support	Lump sum			
4	One time installation, configuration and commissioning as per Annexure-3	Lump sum			
				GRAND TOTAL AMOUNT IN Rs.	

Grand Total Amount in Words Rs.: ____

Note: 1. ***Prices quoted are for scope as mentioned in Annexure 3 and for period of 3 years.***
2. The prices are valid for 180 days from the date of bid.
3. The Basic Price will be considered for final evaluation of the price bid as per BoQ

For and on behalf of:

Signature (Authorized Representative and Signatory of the Bidder):
Name of the Person:
Designation:
Date:

23 ANNEXURE – 5

DETAILS FOR E-TENDER PROCEDURE

NOTICE DETAILS

Tender Reference no.	NOTICE No.: MPCB/EIC/B-200916-FTS-0012 Date: 16/09/2020
Name of Work / Item	Selection of Solution Provider (SP) for Supply, Installation, Commissioning and Support of Integrated IT Security solution at MPCB
Tender Fee	Rs. 5,000/- (Rupees Five Thousand Only) (Non-Refundable) to be paid through Online Payment Modes i.e. Net Banking only, during Tender Document Download Stage.
Pre-bid Meeting	Date 28/09/2020 15:00 PM on Teams or WebEX Platform.
Venue of online opening of tender	MPCB Conference Hall, Kaptaru point, 4th floor Opp, PVR Cinema (near Sion Circle) Sion (East) Mumbai-400 022
Address for Communication	MPCB Conference Hall, Kaptaru point, 4th floor Opp, PVR Cinema (near Sion Circle) Sion (East) Mumbai-400 022
Contact Telephone & Fax Numbers	Tel. No-022-24087295, 022-24010437 Fax-022-24087295
e-Tendering Helpline Support:	**24 X 7 Help Desk Toll Free No.1800 3070 2232 Mobile No. 7878007972, 7878007973, 7878007974.**

e-TENDER TIME SCHEDULE

Please Note: All bid related activities (Process) like Tender Document Download, Bid Preparation, and Bid Submission will be governed by the time schedule given under Key Dates below:

Sr. No.	Activity	Performed by	Start		Expiry	
			Date	From Time	Date	To Time
1	**Release of E-tender**	**Department**	17/09/2020	11:00	17/09/2020	17:00
2	**E-tender Download**	**Bidders**	17/09/2020	11:00	30/09/2020	17:00
3	**Receipt of queries from bidders for Pre-bid**	**Bidders**	17/09/2020	11:00	25/09/2020	17:00
4	**Pre-bid Meeting**	**Department**	28/09/2020 @ 15:00 Hrs			
5	**Bid Submission**	**Bidders**	05/10/2020	11:00	10/10/2020	17:00
6	**Envelope-1 Opening Date (Technical Bid)**	**Department**	13/10/2020	11:00	13/10/2020	15:30
7	**Envelope-2 Opening Date (Price Bid)**	**Department**	**To be announced later**			

** Dates mentioned here, are scheduled dates for Bid Opening Activities***.** *Any changes in dates of opening of technical and commercial bids shall be notified in ‘Press Notice / Corrigendum’ section on the e-Tendering sub portal of the department before opening of the same.*

INSTRUCTIONS TO BIDDERS FOR e-Tendering

GENERAL INSTRUCTIONS:

The bidders are requested to familiarize themselves with the use of the e-Tendering portal of Government of Maharashtra well in advance

To view- Tender Notice, Detailed Time Schedule, Tender Document and BoQ for this Tender and subsequently purchase the Tender Document and its supporting documents, kindly visit following e-Tendering website of **Government of Maharashtra** www.mahatenders.gov.in

All bidders interested in participating in the online e-Tendering process are required to procure Class II or Class III Digital e-Token having 2 certificates inside it, one for Signing/Verification purpose and another for Encryption/Decryption purpose. The tender should be prepared & submitted online using individual's Digital e-Token.

The Contractors participating first time for e-Tenders on Maha e-tendering portal will have to complete the Online Registration Process for the e-Tendering portal. A link for enrolment of new bidders are as follows.
https://mahatenders.gov.in/nicgep/app;jsessionid=CA1444774BB4186D0E04B4178D5CA501.mhgeps2?page=BiddersManualKit&service=page

Empanelment: The Contractors interested in participating in the Tenders of Maharashtra Pollution Control Board processed using the Electronic Tendering System shall be required to enroll on the Electronic Tendering System to obtain Login ID and password.
The Contractors may obtain the necessary information on the process of enrolment either from Helpdesk support team or enrolled directly on Web site www.mahatenders.gov.in.

e-Tendering Tool Kit for Bidders
(detailed Help documents, designed for bidders) has been provided on Mahaetender website in https://mahatenders.gov.in/nicgep/app;jsessionid=CA1444774BB4186D0E04B4178D5CA501.mhgeps2?page=BiddersManualKit&service=page order to guide them through different stages involved during e-Tendering such as online procedure for Tender Document Purchase, Bid Preparation, Bid Submission.

Bidders will have to pay cost of Tender Document through online modes of payment by **Net Banking only** during **Tender Document Download stage**. This payment will not be accepted by the department through any offline modes such as Cash, Cheque or Demand Draft.

Similarly, Bidders will have to pay Earnest Money Deposit through online mode by Net banking only during **Bid Preparation stage**. This payment will not be accepted by the department through any offline modes such as Cash, Cheque or Demand Draft.

For any assistance on the use of Electronic Tendering System, the Users may call the below numbers:-
25 X 7 Help Desk Toll Free No.1800 3070 2232 Mobile No. 7878007972, 7878007973, 7878007974.

For a bidder, online bidding process consists of following 3 stages:

1. *Online Tender Document Purchase and Download*
2. *Online Bid Preparation*
3. *Online Bid Submission*

All of 3 stages are mandatory in order for bidders to successfully complete Online Bidding Process.

ONLINE TENDER DOCUMENT PURCHASE AND DOWNLOAD:

The tender document is uploaded / released on Mahaetenders website www.mahatenders.gov.in Tender document and supporting documents may be purchased and downloaded from above link of Mahaetender site GoM, by making payment through **Online Payment Modes i.e. Net Banking Only.**

If for any reason a bidder fails to make this payment through online modes, system won't allow the bidder proceed further for next stage resulting in his/her elimination from Online Bidding Process.

This payment will not be accepted by the department through any offline modes such as Cash, Cheque or Demand Draft.

Subsequently, bid has to be prepared and submitted online ONLY as per the schedule.

The Tender form will be available online only. Tender forms will not be sold / issued manually. The bidders are required to download the tender document within the pre-scribed date & time mentioned in online tender schedule. After expiry of the date and time for tender document download, Department / Corporation will not be responsible for any such failure on account of bidders for not downloading the document within the schedule even though they have paid the cost of the tender to the Department / Corporation. In such case the cost of the tender paid by the bidders will not be refunded.

PREPARATION & SUBMISSION OF BIDS

Bids shall have to be prepared and subsequently submitted online only. Bids not submitted online will not be entertained.

Online Bid Preparation Price BID

All commercial offers must be prepared online in given BoQ format (An online form will be provided for this purpose in Online Price Bid Envelope during **Online Bid Preparation** stage).

Online Bid Submission

In this stage, bidders who have successfully completed their Bid Preparation stage are required to submit the bid in prescribe time schedule.

INSTRUCTION TO BIDDERS FOR ONLINE BID PREPARATION & SUBMISSION

Bidders are required to pay Earnest Money Deposit (if applicable to them) through online Payment modes i.e. **Net Banking only** during Bid Preparation Stage.

If for any reason a bidder fails to make this payment through online modes, system won't allow the bidder to complete Bid Preparation stage resulting in his/her elimination from Online Bidding Process.

Hence, it is strongly recommended to bidders to initiate this payment well in advance prior to expiry of Bid Preparation stage in order to avoid elimination from Online Bidding Process on grounds of failure to make this payment.

During the activity of **Bid Preparation**, bidders are required to upload all the documents of the technical bid by scanning the documents and uploading those in the PDF format. This apart, bidders will have to quote commercial offer for the work / item as per the format given, for which bids are invited, in an online form made available to them in Commercial Envelope. This activity of **Bid Preparation** should be completed within the pre-scribed schedule given for bid preparation.

After **Bid Preparation**, the bidders are required to complete **Bid Submission** activity within prescribed schedule without which the tender will not be submitted.

The date and time for online preparation followed by submission of envelopes shall strictly apply in all cases. The tenderers should ensure that their tender is prepared online before the expiry of the scheduled date and time and then submitted online before the expiry of the scheduled date and time. No delay on account of any cause will be entertained. Offers not submitted online will not be entertained.

If for any reason, any interested bidder fails to complete any of online stages during the complete tender cycle, department shall not be responsible for that and any grievance regarding that shall not be entertained.

Any amendment to the tender will be placed on sub portal of the Department, who have invited the bids, on Maha e-tendering portal. The tenderer will not be communicated separately regarding the amendment.

OPENING OF BIDS:

The bids that are submitted online successfully shall be opened online as per date and time given in detailed tender schedule (if possible), through e-Tendering procedure only in the presence of bidders (if possible). Bids shall be opened either in the presence of bidders or its duly uthorized representatives. The bidder representatives who are present shall sign a register evidencing their attendance. Only one representative per applicant shall be permitted to be present at the time of opening the tender.

TECHNICAL BID ENVELOPE

This envelope shall be opened online as per the date and time given in detailed tender schedule (if possible), through e-Tendering procedure only,

PRICE BID ENVELOPE:

This envelope shall be opened online as per the date and time given in detailed tender schedule (if possible), through e-Tendering procedure only

Final List of Documents to be uploaded Online:

The following documents should be uploaded by the bidders in the form of PDF Files in the same order as mentioned below, on the e-Tendering website during **Online Bid Preparation** stage.

Sr. No.	List of Documents	Compulsory / Additional
	FOR TECHNICAL BID	
1	Covering Letter As per Format in EXHIBIT 1	Compulsory
2	Attested copy of Power of Attorney	Compulsory
3	Proof of Purchase of RFP	Compulsory
4	EMD as per Section 6.6.2	Compulsory
5	Certificate of incorporation / GST registration certificate	Compulsory
6	Documentary Proofs as testimony for Evaluation of Technical bids as per criteria listed in Section 7.4.1	Compulsory
7	Documentary Proof for establishing minimum Eligibility as mention in Section 7.2 Part1, Technical Proposal as mentioned in section 7.2 PART 2 (b)	Compulsory
8	Covering Letter As per Format in EXHIBIT 2	Compulsory
9	Manufacturer’s Authorisation Form as per EXHIBIT 3	Compulsory
11	Duly filled Technical Compliance form as per Annexure 2	Compulsory
	FOR COMMERCIAL / PRICE BID	
1	**BoQ as per attached in Excel format**	Compulsory
2	Covering Letter As per Format in EXHIBIT 2	Compulsory
3	Price Bid in the format given in Annexure 4, duly signed, sealed	Compulsory

Note: *During **Online Bid Preparation**, apart from the above mentioned documents, if any need arises to upload additional documents in Technical Envelope, an option of ‘**Upload Additional Documents**’ has been provided in the e-Tendering software which will be available to bidders during **Online Bid Preparation** stage.*