RFP Reference Bid No.: *GEM/2023/B/4160916* dated November 02, 2023

Request for Proposal (RFP) for

Procurement and Implementation of Virtual (Software-based) Web Application Firewall (WAF).

The replies to the pre-bid queries received from the prospective bidders for the Pre-Bid Meeting held on November 09, 2023, are placed herewith.

Pre-Bid Queries from Prospective Bidder - 1				
Sl. No.	**Reference**	**Existing RFP Clause**	**Change Request/Suggested Changes**	**Reply to the Query**
1	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. **Suggested Clause:** **The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM**	Necessary corrigendum will be issued
2	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **The solution should be able to protect against API attacks**	Necessary corrigendum will be issued
3	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform S. No. 22	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued

4	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued
5	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **WAF should have controls for Anti Web Defacement**	Necessary corrigendum will be issued
6	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. **Suggested Clause:** **The proposed software should be EAL2 certified**	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 2

Sl No.	Page No/Para No/Sr.No of Tender Document	RFP clause	Amendment Requested	Reason for request of Amendment	Reply to Query
1	Page no.29/Payment terms	After sign-off/go-live. Bank will provide sign-off subject to verification of compliance by its technical consultant/ Experts /IS Auditors of all technical requirements as mentioned in the RFP vis-à-vis what is in the implemented WAF solution. 80% of Total Solution & Implementation Cost.This payment shall be released after the mentioned compliance has been met. At the end of 2nd year and 3rd year : Remaining 10% of Total Solution & Implementation Cost on each of 2nd & 3rd year	After sign-off/go-live. Bank will provide sign-off subject to verification of compliance by its technical consultant/ Experts /IS Auditors of all technical requirements as mentioned in the RFP vis-à-vis what is in the implemented WAF solution. 90% of Total Solution & Implementation Cost.This payment shall be released after the mentioned compliance has been met. 10% could be released after implementation of solution upon submission of 3% Bank Guarantee (BG) of equivalent amount valid till the completion of warranty period with additional claim period of another 6 months)	Being Industry standrad payment terms pertains to Govt.organizations/BFSI,payment terms should be amended as per request of MSME organizations.	Please be guided by the RFP terms and conditions.
2	Page no. 27/Project Implementation Schedule	Solution Delivery:Within 1 week from the date of work order. Implementation, Go-Live,Documentation, SOP & Training - Within 3 weeks form the date of work order On-site support.To start immediately after sign-off for a period of 1 month.	Solution Delivery:Within 2 week from the date of work order. Implementation, Go-Live,Documentation, SOP & Training - Within 4 weeks form the date of work order On-site support.To start immediately after sign-off for a period of 1 month.	Being Enterprise class of products and services only back to back delivery arrangments is applicable from all leading OEMs i.e.4-6 weeks therefore we request to amend the said Delivery and Implementation clause as requested	Please be guided by the RFP terms and conditions.
3	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC.	**Suggested Clause:** The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM	Necessary corrigendum will be issued
4	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution.	**Suggested Clause:** The solution should be able to protect against API attacks	Necessary corrigendum will be issued

5	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 22	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution.	Suggested Clause: Delete the clause+D9:D10	Necessary corrigendum will be issued
6	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution.	**Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued
7	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution.	**Suggested Clause:** WAF should have controls for Anti Web Defacement	Necessary corrigendum will be issued
8	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification.	**Suggested Clause:** The proposed software should be EAL2 certified	Please be guided by the RFP terms and conditions.
9	Generic	Additional Query	To run the Solution any Virtual machine,Hardware /Software, Hypervisor,VM lics.will be in Bidder scope or customer scope !	Request for the clarification	VM Licenses are in the scope of Bank

Pre-Bid Queries from Prospective Bidder - 3			
5.1. Purpose/Objective: Page No. 20		**Clarification Required**	**Reply to the Query**
	a) To supply and implement software-based Web Application Firewall (WAF) with a centralized dashboard that should provide real time incident response, reporting and monitoring.	We request NHB to allow Cloud bases SAAS solution	Please be guided by the RFP terms and conditions.
	b) The minimum application throughput WAF must be 200 Mbps and support minimum 50 websites/applications.	Why is Bank looking to limit the bandwidth? In case of DDOS attacks 1gbps is very common traffic, with limiting the bandwidth NHB applications will be dwon in case of DDOS attck reaching beyond 200 mbps	Please be guided by the RFP terms and conditions.
	c) To set up a Solution which would have a vulnerability scanner and/or support integration with 3rd party vulnerability scanners.	NHB must also ask to give quick WAF Rules compatibiloity detail in report on how many Vulnerabilities are by default address by WAF and how many can be managed by writing new custom rules (as soon as scaning report comes)	Please be guided by the RFP terms and conditions.
		OEM must take ownership of custom rules with SLA to write the custom rules for newly identified vulnerability within 24 hours for critical vulnerabilities, We request NHB to include clause of SLA by OEM to get best utilisation of WAF and protection of NHB websites	Please be guided by the RFP terms and conditions.
	e) Solution which should be able to evaluate and classify security-policy compliance by user, device, location, operating system, and other criteria.	The custom WAF policies can be defined based on parameters such as session, user agent, Geo Location etc. Request you to elaborate the requirement for user, device and operating system.	Please be guided by the RFP terms and conditions.
	f) Must have pre-admission and post-admission access control.	We assume this is regarding the RBAC access for WAF reporting portal. Kindly confirm.	Please be guided by the RFP terms and conditions.
4	Present Set-Up c) Public Facing websites are hosted at Bank's DC/DR/vendor's DC. At present, Bank has around 20 applications including 15 public facing.	As mentioned, Bank has 20 Applications. Out of which 15 public facing, kindly confirm the type of rest 5 Applications. Hope these 5 Applications are also reachable through internet.	Others are intranet based
	Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform		
	5. The solution should provide security against advanced threat vectors like BOT virus mitigation, Layer7 Distributed Denial of Service, and credential protection.	We assume the requirement here is for BOT Attack Protection in reference to BOT virus mitigation. Kindly confirm.	Yes
	9 The solution should also support sending of logs in CEF/syslog/CSOC/Manage Engine etc.	In case APIs are provided to pull the logs in JSON format will it suffice the requirement? Kindly confirm.	yes
	13. The solution must be able to identify Web Socket connections.	The requirement here is to support Web Socket traffic or to identify Web Sockets in Application. Kindly confirm.	To Identify Web Socket Connection
	18. The proposed system should provide configuration options for preventing fingerprinting of system generated cookies and parameters	Please elaborate the requirement in more detail.	Session management, unique session Id, visitor identification, Age of Cookie, Identifying Browser and other configuration options related to fingerprinting
	20. The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint.	Please elaborate the requirement for API Gateway.	Necessary corrigendum will be issued
5.2. Statement of Work: Page No.21			
	The solution must be VM based (Virtualized) and equipped with inbuilt software configurations for web application. The VM has to be supported on major virtualization platforms e.g. VMware & Hyper-V.	We request NHB to consider SAAS - Cloud based solution where, OEM must take responsibility of Infra management & solution as well	Please be guided by the RFP terms and conditions.

	Solution will be in high availability at Bank's DC (Active – Passive or Active - Active) and standalone device at DR but with potential to implement the same configurations at both DC and DR.	WAF on Cloud as SAAS is best and is highly Available and scalable model, DC & DR of Bank can be managed very easily, We request NHB to consider allowing SAAS based WAF, more than infra focused NHB should be considering Uptime SLA focused	Please be guided by the RFP terms and conditions.
	The implementation will be carried out at DC & DR sites as per the terms of RFP .	SAAS model deployment can be done with zero downtime wihout any installation at customer environment, We request HNB to allow Cloud based WAF	Please be guided by the RFP terms and conditions.
	Virtual CPU Cores		
	RAM 6 GB, 6 Cores, Disk Space 50 GB, VMware/Hyper- V	whatever Size in considered, it will manage Application level DDOS upto that limited extent only, With Cloud Based SAAS NHB can achieve unlimited unmetered DDOS protection.	Please be guided by the RFP terms and conditions.
Annexure D: Minimum Eligibility Criteria: Page No. 40. Point no. 7	The proposed WAF solution must be listed in either the Gartner Magic's quadrant OR Forrester Wave Report for Web Application Firewall/WAAP solution in any one of the last two years [2022 or 2023] Gartner/Forrester report to be submitted having clear mention of the proposed solution	NHB should concider Gartner's peer Insight Review in place of Gartner MQ, as no Gartner MQ has be released in 2023, and its been replaced by Gartner's Peer Insight Review now, Peer Insight review system is reviews only form user/customer of the product and only a customer can give review of respective product. https://www.gartner.com/reviews/market/cloud-web-application-and-api-protection	Necessary corrigendum will be issued

Pre-Bid Queries from Prospective Bidder - 4			
Reference	**RFP clause**	**Amendment Requested**	Reply
(Annexure 'D'- (Minimum Eligibility Criteria)	The Bidder should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs.	It is better to include in the eligibility criteria for PO that Bidder should have experience of supplying, deploying, implementing, managing & monitoring complete IT Infra solutions/ services which includes networks, servers, desktops, Browsers, mobile devices, Active Directory, and security etc. along with applications. Bidders should have in-depth visibility/understanding of the network and have control over it by detecting network faults or unusual behavior in real time with the help of any monitoring software. Having exposure/experience to all these with Bidders shows that they understand the entire IT Network environment either it is LAN, WAN OR a DMZ or demilitarized zone (It is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet) and are capable to manage the same.	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder - 5				
Sl. No.	**Reference**	**Existing RFP Clause**	**Change Request/Suggested Changes**	Reply to the Query
1	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. **Suggested Clause:** **The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM**	Necessary corrigendum will be issued
2	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **The solution should be able to protect against API attacks**	Necessary corrigendum will be issued
3	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued

4	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued
5	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **WAF should have controls for Anti Web Defacement**	Necessary corrigendum will be issued
6	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. **Suggested Clause:** **The proposed software should be EAL2 certified**	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 6					
Sr. No	**RFP Page**	**Point**	**Description**	**Clarification**	**Reply to the Query**
1	21	5.2 -Statement of work	Bidder should provide extensive WAF administration and troubleshooting hands on training to Bank's NOC team. Trainings shall be imparted as per the industrial standard.	Need to know the Training method - Virtual /on prem , Duration, No of persons	Can be virtual/on premises. The details will be shared with the selected bidder
2	21	5.2 -Statement of work	The bidder would train the Bank's personnel for independent operation, creation of policies/rules, generation of reports, analysis of the reports, correlation with other relevant security related applications/events, familiarization of features and functionalities	Need to know the Training method - Virtual /on prem , Duration, No of persons	Can be virtual/on premises. The details will be shared with the selected bidder
3	22	5.2 -Statement of work	The successful bidder shall handle all matters including the configuration, operation, monitoring, management, and maintenance of the software/solution including but not limited to application, system interfaces etc.	Need to know the duration for this as the RFP is not asking for a onsite engineer	Refer following RFP clause The Bidder shall engage one onsite Engineer for a period of 1-month w.e.f. the date of Go-Live. "Bidder's expert team will be onsite till complete installation, implementation, and project signoff.
4	22	5.2 -Statement of work	Any other software component including OS (except Windows Server), webserver, database etc. required in connections with the work will be supplied and installed by the bidder.	Need to know the requirements - Webserver for clarity & also if the addl hardware is supplied whether the Rackspace and power would be provided by NHB	Will be discussed with successful bidder
5	25	10. Penalty for Implementation	If not implemented within 3 weeks from the date of acceptance of work order, 1 % of the Total Solution & Implementation Cost /week subject to maximum of 10% of the Total Solution Cost, will be levied as penalty	Kindly cosider the caping for the supply of the Material and implementation cost for the Implementation penalty	Please be guided by the RFP terms and conditions
6	26	10.1 Penalty for Downtime	Penalties, subject to maximum of 10% of Total Solution & Implementation Cost in any year, will be deducted from the next due payment or if the maximum penalty limit has been reached, the subsequent penalties will be deducted from the PBG.	Kindly cosider the caping for support cost downtime penalty	Please be guided by the RFP terms and conditions
7	27	10.2 Penalty for resolution		Kindly cosider the caping for support cost downtime penalty	Please be guided by the RFP terms and conditions
8	27	11 1-Project Implementation Schedule -Solution Delivery	Within 1 week from the date of work order.	Provide us with 4 weeks for Delivery from Podate	Please be guided by the RFP terms and conditions

9	27	11- 2 -Implementation, Go-Live, Documentation, SOP & Training	Within 3 weeks form the date of work order	Provide us with 8 weeks from the Po date	Please be guided by the RFP terms and conditions
10	24	8 -Audit Requirements	Bank is subjected to various audits [internal / statutory / RBI etc.]. In the event of any observation by the audit regarding security, access etc., the same will be intimated to the Bidder. The Vendor to carry out the changes for enabling Bank to comply on the same, if required. No additional cost would be paid by Bank	The cost of any Hardware/Software as recommended by RBI needs to be borne by NHB .	With respect to WAF solution, the Vendor to carry out the changes for enabling Bank to comply on the same, if required. No additional cost would be paid by Bank
11	23	General Requirement Point J	The Bidder shall engage one onsite Engineer for a period of 1-month w.e.f. the date of Go-Live.	Need to know the qualification/certification/Role and responsibility of the engineer	Experience in WAF implementation.
12		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. **Suggested Clause:** **The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM**	Necessary corrigendum will be issued
13		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **The solution should be able to protect against API attacks**	Necessary corrigendum will be issued

14		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 22	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued
15		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued
16		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **WAF should have controls for Anti Web Defacement**	Necessary corrigendum will be issued

17		RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. **Suggested Clause:** **The proposed software should be EAL2 certified**	Please be guided by the RFP terms and conditions
18					
19			To supply and implement software-based Web Application Firewall (WAF) with a centralized dashboard that should provide real time incident response, reporting and monitoring.	We request NHB to allow Cloud bases SAAS solution	Please be guided by the RFP terms and conditions
20			The minimum application throughput WAF must be 200 Mbps and support minimum 50 websites/applications.	Why is Bank looking to limit the bandwidth? In case of DDOS attacks 1gbps is very common traffic, with limiting the bandwidth NHB applications will be dwon in case of DDOS attck reaching beyond 200 mbps	Please be guided by the RFP terms and conditions
21			To set up a Solution which would have a vulnerability scanner and/or support integration with 3rd party vulnerability scanners.	NHB must also ask to give quick WAF Rules compatibiloity detail in report on how many Vulnerabilities are by default address by WAF and how many can be managed by writing new custom rules (as soon as scaning report comes)	Please be guided by the RFP terms and conditions
22				OEM must take ownership of custom rules with SLA to write the custom rules for newly identified vulnerability within 24 hours for critical vulnerabilities, We request NHB to include clause of SLA by OEM to get best utilisation of WAF and protection of NHB websites	Please be guided by the RFP terms and conditions
23			Solution which should be able to evaluate and classify security-policy compliance by user, device, location, operating system, and other criteria.	The custom WAF policies can be defined based on parameters such as session, user agent, Geo Location etc. Request you to elaborate the requirement for user, device and operating system.	Please be guided by the RFP terms and conditions
24			Must have pre-admission and post-admission access control.	We assume this is regarding the RBAC access for WAF reporting portal. Kindly confirm.	Please be guided by the RFP terms and conditions
25			Present Set-Up c) Public Facing websites are hosted at Bank's DC/DR/vendor's DC. At present, Bank has around 20 applications including 15 public facing.	As mentioned, Bank has 20 Applications. Out of which 15 public facing, kindly confirm the type of rest 5 Applications. Hope these 5 Applications are also reachable through internet.	Please be guided by the RFP terms and conditions

26			Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform		
27			The solution should provide security against advanced threat vectors like BOT virus mitigation, Layer7 Distributed Denial of Service, and credential protection.	We assume the requirement here is for BOT Attack Protection in reference to BOT virus mitigation. Kindly confirm.	Yes
28			The solution should also support sending of logs in CEF/syslog/CSOC/Manage Engine etc.	In case APIs are provided to pull the logs in JSON format will it suffice the requirement? Kindly confirm.	Yes
29			The solution must be able to identify Web Socket connections.	The requirement here is to support Web Socket traffic or to identify Web Sockets in Application. Kindly confirm.	To Identify Web Socket Connection
30			The proposed system should provide configuration options for preventing fingerprinting of system generated cookies and parameters	Please elaborate the requirement in more detail.	Session management, unique session Id, visitor identification, Age of Cookie, Identifying Browser and other configuration options related to fingerprinting
31			The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint.	Please elaborate the requirement for API Gateway.	Necessary corrigendum will be issued
32			The solution must be VM based (Virtualized) and equipped with inbuilt software configurations for web application. The VM has to be supported on major virtualization platforms e.g. VMware & Hyper-V.	We request NHB to consider SAAS - Cloud based solution where, OEM must take responsibility of Infra management & solution as well	No change in deployment model
33			Solution will be in high availability at Bank's DC (Active – Passive or Active - Active) and standalone device at DR but with potential to implement the same configurations at both DC and DR.	WAF on Cloud as SAAS is best and is highly Available and scalable model, DC & DR of Bank can be managed very easily, We request NHB to consider allowing SAAS based WAF, more than infra focused NHB should be considering Uptime SLA focused	No change in deployment model
34			The implementation will be carried out at DC & DR sites as per the terms of RFP .	SAAS model deployment can be done with zero downtime wihout any installation at customer environment, We request HNB to allow Cloud based WAF	No change in deployment model
35			**Virtual CPU Cores**		
36			RAM 6 GB, 6 Cores, Disk Space 50 GB, VMware/Hyper- V	whatever Size in considered, it will manage Application level DDOS upto that limited extent only, With Cloud Based SAAS NHB can achieve unlimited unmetered DDOS protection.	No change in deployment model

37			The proposed WAF solution must be listed in either the Gartner Magic's quadrant OR Forrester Wave Report for Web Application Firewall/WAAP solution in any one of the last two years [2022 or 2023] Gartner/Forrester report to be submitted having clear mention of the proposed solution	Request to NHB should concider Gartner's peer Insight Review in place of Gartner MQ, as no Gartner MQ has be released in 2023, and its been replaced by Gartner's Peer Insight Review now, Peer Insight review system is reviews only form user/customer of the product and only a customer can give review of respective product.	Necessary corrigendum will be issued

Pre-Bid Queries from Prospective Bidder - 7					
Sl No	**Page No**	**Clause No**	**RFP Clause**	**Query**	**Reply**
1	8	1.2 Bid Summary	Earnest Money Deposit (EMD) Amount EMD of Rs. 3,00,000/-	We would like to inform you that, as per your tender terms and condition and GEM GTC (link is given in the bid document and clause is mentioned at pg. no. 17 & clause no. m (v), it is mentioned there that Sellers will get exemption from furnishing Bid Security Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s). https://assets-bg.gem.gov.in/resources/upload/shared_doc/gtc/General-Te-1692264494.pdf We hereby inform you that in Financial Year 2022-23, the turnover of our company is Rs. 603.063 Crores. On the basis of above-mentioned points in tender document and GEM GTC guidelines, we are eligible to claim EMD exemption in this tender. We request you to kindly confirm on the acceptance of above mentioned GEMs terms & conditions.	Please be guided by the RFP terms and conditions
	27	11. Project Implementation Schedule	The Vendor shall be required to deliver and implement the solutions as per following timelines, failing which penalty/LD (Liquidated Damages) as applicable shall be levied: Solution Delivery Within 1 week from the date of work order.	Solution Delivery: Within 8 to 10 week from the date of work order.	Please be guided by the RFP terms and conditions
	29	17. Payment Terms	After sign-off/go-live. Bank will provide sign-off subject to verification of compliance by its technical consultant/ Experts /IS Auditors of all technical requirements as mentioned in the RFP vis-à-vis what is in the implemented WAF solution. 80% of Total Solution & Implementation Cost. This payment shall be released after the mentioned compliance has been met.	80% on Delivery 10% After Implementation Additional 10% payment within 2 month of implementation by submitting PBG of same value.	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder - 8					
#	**Bid Document Reference (Volume, Section No.)**	**Page Number**	**Content of the bid requiring clarification**	**Clarification Sought/Query**	**Remarks**
1	3.12 Performance Guarantee	13	As per GeM. The selected Bidder will be required to provide a performance bank guarantee/PBG for 6% of Total Solution & Implementation Cost as Performance Guarantee (Format at Annexure 'L'), in the form of bank guarantee from a Scheduled Commercial Bank. For future requirement, Bidder will be required to separately provide a performance bank guarantee/PBG for 6% of total future cost. PBG for the additional procurement/extended support shall be furnished separately equivalent to 6% of such total cost.	We request you to consider Performance Bank Guarantee for a value equivalent to **3%** of the Total Solution & Implementation Cost .	Please be guided by the RFP terms and conditions.
2	17. Payment Terms, Sr. No. - 1	29	After sign-off/go-live. Bank will provide sign-off subject to verification of compliance by its technical consultant/ Experts /IS Auditors of all technical requirements as mentioned in the RFP vis-à-vis what is in the implemented WAF solution. - 80% of Total Solution & Implementation Cost.	We request you to change the Payment Terms as below: 1. Delivery of Software - **70%** 2. Instalaltion & Comissioning - **10%** 3. Sign-off & Go-Live - **10%**	Please be guided by the RFP terms and conditions.
3	17. Payment Terms, Sr. No. - 2	29	At the end of 2nd year and 3rd year - Remaining 10% of Total Solution & Implementation Cost on each of 2nd & 3rd year	We request you to change the Payment Terms as below: "At the end of 2nd year and 3rd year - Remaining **5%** of Total Solution & Implementation Cost on each of 2nd & 3rd year"	Please be guided by the RFP terms and conditions.
4	Annexure 'D'- (Minimum Eligibility Criteria), Sr. No. 5	41	The Bidder should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs.	We request you to change the Eligibility Criteria as below: "The Bidder **/ OEM** should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs."	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 9				
S.No.	**RFP Reference Section**	**RFP Reference Page**	**Points of clarification required**	**Reply to query**
1	Page 89 / WAF Technical Specification / point 41	Page 89	Web applications are #1 source of security breaches. We recommend to add the following clause in WAF. Suggestive Clause The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc.	Can be provided with the proposed solution.
2	Page 89 / WAF Technical Specification / point 20	Page 89	Company want to integrate the threat feed from other resources to protect the organsation and infra as well. We recommend to add the following clause in WAF. Suggestive Clause The proposed solution should have 3rd party threat feed integration to allow bulk IP blacklisting using API, FTP and schedule task etc.	Can be provided with the proposed solution.
3	Page 89 / WAF Technical Specification / point 23	Page 89	As the solution is going to integrate with service mesh environment, we assume that some of the applications are going to be API first applications. In order to adequately protect APIs from Layer 7 DDoS attacks without impacting API queries from legitimate users, we recommend to add the following clause in WAF. Suggestive Clause The solution should client SDK for web and mobile clients from same OEM for additional layer of security against attacks targeting API infrastructure.	Can be provided with the proposed solution.
4	Page 89 / WAF Technical Specification / point 28	Page 89	According to the custom business requirement, it should be able to allow or block traffic and mitigate application requests. We recommend adding the following clause to the WAF. Suggestive Clause The proposed solution for user defined variables and scripts for building custom application specific security policy.	Can be provided with the proposed solution.

Pre-Bid Queries from Prospective Bidder - 10				
Sl. No.	**Reference**	**Existing RFP Clause**	**Change Request/Suggested Changes**	**Reply to the Query**
1	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. **Suggested Clause:** **The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM**	Necessary corrigendum will be issued.
2	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **The solution should be able to protect against API attacks**	Necessary corrigendum will be issued.
3	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 22	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued.
4	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued.
5	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **WAF should have controls for Anti Web Defacement**	Necessary corrigendum will be issued.
6	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. **Suggested Clause:** **The proposed software should be EAL2 certified**	Please be guided by the RFP terms and conditions.

7	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure D - (Minimum Eligibility Criteria) - Point no. 5	The Bidder should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs.	The Bidder/OEM should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs. OR We suggest the clause as Bidder having any atleast 1 WAF PRoject in Govt/PSU/Bank with onging project of value of 3 CR. This is new technology and there are very limited implementation of such technology	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 11						
Sr. No.	**Page No.**	**Section**	**Clause No.**	**RFP Text**	**Query/Suggestion for Amendment**	**Reply to the Query**
1	27	Project Implementation Schedule	10	Implementation, Go-Live, Documentation, SOP & Training Within 3 weeks form the date of work order	Kindly allow at least 6 weeks form the date of work order Go-Live, (3 weeks for delivery of solution + 3 weeks for Implementation, Go-Live, Documentation, SOP & Training.	Please be guided by the RFP terms and conditions
2	29	Payment Terms	17	After sign-off/go-live - 80% of Total Solution & Implementation Cost. At the end of 2nd year and 3rd year - Remaining 10% of Total Solution & Implementation Cost on each of 2nd & 3rd year	We request NHB to kindly amend the payment terms as follows: 80% on delivery of solution 10% on Implementation, Go-Live, Documentation, SOP & Training Remaining 10% of Total Solution & Implementation Cost at the beginning of 2nd and 3rd year	Please be guided by the RFP terms and conditions
3	25	Penalty for Delay in Implementation	10	If not implemented within 3 weeks from the date of acceptance of work order, 1 % of the Total Solution & Implementation Cost /week subject to maximum of 10% of the Total Solution Cost, will be levied as penalty.	We request NHB to kindly amend the clause as follows: If not implemented within 6 weeks from the date of acceptance of work order, 0.5 % of the Total Solution & Implementation Cost /week subject to maximum of 5% of the Total Solution Cost, will be levied as penalty.	Please be guided by the RFP terms and conditions

4	26	Penalty for Downtime	10.1	98% to < 99.5% - Rs 10,000/- Below 98.00% - Rs. 50,000/ per 1% of drop in uptime	Kindly amend the downtime penalty as follows: 98% to < 99.5% - Rs 5,000/- Below 98.00% - Rs. 10,000/ per 1% of drop in uptime	Please be guided by the RFP terms and conditions
5	40	Annexure 'D'- (Minimum Eligibility Criteria)	All Eligibility Criteria	All Eligibility Criteria	We request NHB to add the following clause against all qualifying criteria: "In-case of corporate restructuring the earlier/parent entity's incorporation certificate, financial statements, Experience Credentials, etc. may be considered."	Please be guided by the RFP terms and conditions
6	94	5.2		The details of available infrastructure both at Bank's DC & DR site for WAF VM is as under	With required technical and functional specification, we suggest to have minimum 16 cores CPU, 64GB RAM and 200GB storage. The right VM sizing will help WAF to perform optimally and deliver expected functionalities.	To be discussed with the selected bidder at the time of implementation
7	90	Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	In order to scan for AV locally within appliance and minimal latency in web traffic transaction, the AV database should be inbuilt within appliance with regular updates / enrich from OEM threat cloud. To secure NHB web traffic againt AV and faster response, kindly change the specification as below. "The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against inbuilt AV database."	Necessary corrigendum will be issued.

8	91	Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	31	The Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Various OEM has multiple feature to deliver required technical specification. We request change in the specification for maximum participation and not limiting to specific OEM. "The Proposed solution should have capability to redirect Brute force attack / vulnerabilities traffic to Honey Pot page."	Please be guided by the RFP terms and conditions
9			Additional Points Suggested	Additional Points Suggested	To prevent NHB environment with both known and unknown threats, it is highly recommended to have web application firewall with zero-day analysis appliance. While specification of Zero day appliance is not mentioned in the technical specification, we request to add below points to secure NHB environment against sophisticated threats both known and unknown. 1. "Solution should integrate bidirectional with on-prem Anti-APT. Threat intelligence of WAF and Anti-APT solution should be from same OEM Threat Lake." 2. "Anti-APT solution should process 200 files per hour. Anti-apt solution should be proposed for DC and DR with required VM and OS licenses from day 1"	This can be part of proposed solution. Not a restrcitive clause

Pre-Bid Queries from Prospective Bidder - 12				
Sl. No.	**Reference**	**Existing RFP Clause**	**Change Request/Suggested Changes**	**Reply**
1	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 11	The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM or ADC (Application Delivery Controller).	There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. **Suggested Clause:** **The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM**	Necessary corrigendum will be issued.
2	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 20	The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint	WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **The solution should be able to protect against API attacks**	Necessary corrigendum will be issued.
3	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 22	The WAF should have ability to identify Client site vulnerabilities like presence of a Keylogger & should have mechanism to prevent against it.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued.

4	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **Delete the clause**	Necessary corrigendum will be issued.
5	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform S. No. 25	WAF should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. **Suggested Clause:** **WAF should have controls for Anti Web Defacement**	Necessary corrigendum will be issued.
6	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform	New Clause Request	Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. **Suggested Clause:** **The proposed software should be EAL2 certified**	Please be guided by the RFP terms and conditions.

7	RFP Reference No.: NHB/ITD/RFP-WAF/2023 Request for Proposal (RFP) for Procurement and Implementation of Virtual (Software based) Web Application Firewall (WAF) Annexure D - (Minimum Eligibility Criteria) - Point no. 5	The Bidder should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs.	The Bidder/OEM should have experience in implementing Web Application Firewall (WAF) Solution in at least 2 institutions in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs. OR Bidder should have any ongoing project of value of 3 Cr in India with at-least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates in India during the last 5 FYs.	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 13					
S.No.	**RFP Reference Section**	**RFP Reference Page**	**Content of RFP requiring clarification**	**Points of clarification required**	**Reply**
1	Page 89 / WAF Technical Specification / point 41	Page 89		Web applications are #1 source of security breaches. We recommend to add the following clause in WAF. Suggestive Clause The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc.	Please be guided by the RFP terms and conditions. Not a restrictive clause
2	Page 89 / WAF Technical Specification / point 20	Page 89		Company want to integrate the threat feed from other resources to protect the organsation and infra as well. We recommend to add the following clause in WAF. Suggestive Clause The proposed solution should have 3rd party threat feed integration to allow bulk IP blacklisting using API, FTP and schedule task etc.	Please be guided by the RFP terms and conditions. Not a restrictive clause
3	Page 89 / WAF Technical Specification / point 23	Page 89		As the solution is going to integrate with service mesh environment, we assume that some of the applications are going to be API first applications. In order to adequately protect APIs from Layer 7 DDoS attacks without impacting API queries from legitimate users, we recommend to add the following clause in WAF. Suggestive Clause The solution should client SDK for web and mobile clients from same OEM for additional layer of security against attacks targeting API infrastructure.	Please be guided by the RFP terms and conditions. Not a restrictive clause
4	Page 89 / WAF Technical Specification / point 28	Page 89		According to the custom business requirement, it should be able to allow or block traffic and mitigate application requests. We recommend adding the following clause to the WAF. Suggestive Clause The proposed solution for user defined variables and scripts for building custom application specific security policy.	Please be guided by the RFP terms and conditions. Not a restrictive clause

Pre-Bid Queries from Prospective Bidder - 14		
S No.	**Representations**	**Reply to the Query**
1	After sign-off/go-live. Bank will provide sign-off subject to verification of compliance by its technical consultant/ Experts /IS Auditors of all technical requirements as mentioned in the RFP vis-à-vis what is in the implemented WAF solution. 90% of Total Solution & Implementation Cost.This payment shall be released after the mentioned compliance has been met. 10% could be released after implementation of solution upon submission of 3	Please be guided by the RFP terms and conditions.
2	Solution Delivery:Within 2 week from the date of work order. Implementation, Go-Live,Documentation, SOP & Training - Within 4 weeks form the date of work order On-site support.To start immediately after sign-off for a period of 1 month. Being Enterprise class of products and services only back to back delivery arrangements is applicable from all leading OEMs i.e.4-6 weeks therefore we request to amend the said Delivery and Implementation clause as requested	Please be guided by the RFP terms and conditions.
3	Tech Spec S. No. 11 There are OEM as well who are also leading manufacturer of WAF solution and offer solution as a part of ADC, same solution is deployed across large government banks. Hence, request to ammend the clause to allow participation for ADC manufacturer as well who offer WAF on top of ADC. Suggested Clause: The proposed WAF solution should be on dedicated virtualization environment (supported on both VMware and Hyper-V), it should not be part of any Firewall or UTM	Necessary corrigendum will be issued.
4	Tech Spec S.no.20 WAF is used to protect your hosted application from web attacks, API Gateway should not be asked on WAF. It should be part of dedicated solution. Suggested Clause: The solution should be able to protect against API attacks	Necessary corrigendum will be issued.
5	Tech spec S.no.22 WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. Suggested Clause: Delete the clause	Necessary corrigendum will be issued.
6	Tech Spec. S.no.24 WAF is used to protect your hosted application from web attacks, file inspection should not be asked on WAF. It should be part of dedicated solution. Suggested Clause: Delete the clause	Necessary corrigendum will be issued.
7	Tech Spec S.no.25 WAF is used to protect your hosted application from web attacks, client side protection should not be asked on WAF. It should be part of dedicated solution. Suggested Clause: WAF should have controls for Anti Web Defacement	Necessary corrigendum will be issued.
8	New Clause Request Solution should be stable and reliable to effectively mitigate ongoing attacks, EAL2 certification ensure the same. All leading manufacturer including MII vendor has this certification. Suggested Clause: The proposed software should be EAL2 certified	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 15						
S.No.	**Page No.**	**Section No.**	**Point No.**	**RFP Text**	**Query/Suggestion for Amendment**	**Reply to the Query**
1	94	5.2		The details of available infrastructure both at Bank's DC & DR site for WAF VM is as under	With required technical and functional specification, we suggest to have minimum 16 cores CPU, 64GB RAM and 200GB storage. The right VM sizing will help WAF to perform optimally and deliver expected functionalities.	To be discussed with the selected bidder at the time of implementation
2	90	Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform	24	The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against AV database.	In order to scan for AV locally within appliance and minimal latency in web traffic transaction, the AV database should be inbuilt within appliance with regular updates / enrich from OEM threat cloud. To secure NHB web traffic againt AV and faster response, kindly change the specification as below. "The proposed solution should support scanning for malicious content in uploads along with File upload violations and scan the file against inbuilt AV database."	Necessary corrigendum will be issued.
3	91	Annexure – Solution compliance Statement-WAF Technical Specification on Virtualization Platform	31	The Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Various OEM has multiple feature to deliver required technical specification. We request change in the specification for maximum participation and not limiting to specific OEM. "The Proposed solution should have capability to redirect Brute force attack / vulnerabilities traffic to Honey Pot page."	Please be guided by the RFP terms and conditions
4			Additional Points		To prevent NHB environment with both known and unknown threats, it is highly recommended to have web application firewall with zero-day analysis appliance. While specification of Zero day appliance is not mentioned in the technical specification, we request to add below points to secure NHB environment against sophisticated threats both known and unknown. "Solution should integrate bidirectional with on-prem Anti-APT. Threat intelligence of WAF and Anti-APT solution should be from same OEM Threat Lake." "Anti-APT solution should process 200 files per hour. Anti-apt solution should be proposed for DC and DR with required VM and OS licenses from day 1"	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder - 16			
5.1. Purpose/Objective: Page No. 20		**Clarification Required**	**Reply to the Query**
	a) To supply and implement software-based Web Application Firewall (WAF) with a centralized dashboard that should provide real time incident response, reporting and monitoring.	We request NHB to allow Cloud bases SAAS solution	Please be guided by the RFP terms and conditions.
	b) The minimum application throughput WAF must be 200 Mbps and support minimum 50 websites/applications.	Why is Bank looking to limit the bandwidth? In case of DDOS attacks 1gbps is very common traffic, with limiting the bandwidth NHB applications will be dwon in case of DDOS attck reaching beyond 200 mbps	Please be guided by the RFP terms and conditions.
	c) To set up a Solution which would have a vulnerability scanner and/or support integration with 3rd party vulnerability scanners.	NHB must also ask to give quick WAF Rules compatibiloity detail in report on how many Vulnerabilities are by default address by WAF and how many can be managed by writing new custom rules (as soon as scaning report comes)	Please be guided by the RFP terms and conditions.
		OEM must take ownership of custom rules with SLA to write the custom rules for newly identified vulnerability within 24 hours for critical vulnerabilities, We request NHB to include clause of SLA by OEM to get best utilisation of WAF and protection of NHB websites	Please be guided by the RFP terms and conditions.
	e) Solution which should be able to evaluate and classify security-policy compliance by user, device, location, operating system, and other criteria.	The custom WAF policies can be defined based on parameters such as session, user agent, Geo Location etc. Request you to elaborate the requirement for user, device and operating system.	Please be guided by the RFP terms and conditions.
	f) Must have pre-admission and post-admission access control.	We assume this is regarding the RBAC access for WAF reporting portal. Kindly confirm.	Please be guided by the RFP terms and conditions.
4	Present Set-Up c) Public Facing websites are hosted at Bank's DC/DR/vendor's DC. At present, Bank has around 20 applications including 15 public facing.	As mentioned, Bank has 20 Applications. Out of which 15 public facing, kindly confirm the type of rest 5 Applications. Hope these 5 Applications are also reachable through internet.	Others are intranet based applications
	Annexure – Solution compliance Statement- WAF Technical Specification on Virtualization Platform		
	5. The solution should provide security against advanced threat vectors like BOT virus mitigation, Layer7 Distributed Denial of Service, and credential protection.	We assume the requirement here is for BOT Attack Protection in reference to BOT virus mitigation. Kindly confirm.	Yes

	9 The solution should also support sending of logs in CEF/syslog/CSOC/Manage Engine etc.	In case APIs are provided to pull the logs in JSON format will it suffice the requirement? Kindly confirm.	Yes
	13. The solution must be able to identify Web Socket connections.	The requirement here is to support Web Socket traffic or to identify Web Sockets in Application. Kindly confirm.	To Identify Web Socket Connection
	18. The proposed system should provide configuration options for preventing fingerprinting of system generated cookies and parameters	Please elaborate the requirement in more detail.	Session management, unique session Id, visitor identification, Age of Cookie, Identifying Browser and other configuration options related to fingerprinting
	20. The solution should be able to act as an API Gateway with options to configure API User, API Key Authentication & Rate Limiting requests to protected API Endpoint.	Please elaborate the requirement for API Gateway.	Necessary corrigendum will be issued.
5.2. Statement of Work: Page No.21			
	The solution must be VM based (Virtualized) and equipped with inbuilt software configurations for web application. The VM has to be supported on major virtualization platforms e.g. VMware & Hyper-V.	We request NHB to consider SAAS - Cloud based solution where, OEM must take responsibility of Infra management & solution as well	Please be guided by the RFP terms and conditions.
	Solution will be in high availability at Bank's DC (Active – Passive or Active - Active) and standalone device at DR but with potential to implement the same configurations at both DC and DR.	WAF on Cloud as SAAS is best and is highly Available and scalable model, DC & DR of Bank can be managed very easily, We request NHB to consider allowing SAAS based WAF, more than infra focused NHB should be considering Uptime SLA focused	Please be guided by the RFP terms and conditions.
	The implementation will be carried out at DC & DR sites as per the terms of RFP .	SAAS model deployment can be done with zero downtime wihout any installation at customer environment, We request HNB to allow Cloud based WAF	Please be guided by the RFP terms and conditions.
	Virtual CPU Cores		
	RAM 6 GB, 6 Cores, Disk Space 50 GB, VMware/Hyper- V	whatever Size in considered, it will manage Application level DDOS upto that limited extent only, With Cloud Based SAAS NHB can achieve unlimited unmetered DDOS protection.	Please be guided by the RFP terms and conditions.

Annexure D: Minimum Eligibility Criteria: Page No. 40. Point no. 7	The proposed WAF solution must be listed in either the Gartner Magic's quadrant OR Forrester Wave Report for Web Application Firewall/WAAP solution in any one of the last two years [2022 or 2023] Gartner/Forrester report to be submitted having clear mention of the proposed solution	NHB should concider Gartner's peer Insight Review in place of Gartner MQ, as no Gartner MQ has be released in 2023, and its been replaced by Gartner's Peer Insight Review now, Peer Insight review system is reviews only form user/customer of the product and only a customer can give review of respective product. https://www.gartner.com/reviews/market/cloud-web-application-and-api-protection	Necessary corrigendum will be issued.

Pre-Bid Queries from Prospective Bidder - 17	
Query	**Reply to the Query**
We would like to request you to please allow us Joint Venture	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder - 18				
S.NO	**Reference**	**Existing RFP Clause**	**Change Request/Suggested Changes**	**Reply to the Query**
1.	The proposed WAF solution must be listed in either the Gartner Magic's quadrant OR Forrester Wave Report for Web Application Firewall/WAAP solution in any one of the last two years [2022 or 2023]	Gartner/Forrester report to be submitted having clear mention of the proposed solution	Attached the Indian Government office memorandum dated December 20th, 2022. This document highlights examples of "Restrictive and discriminatory conditions against the local suppliers" as well as "Other conditions which make the bid noncompliant to PPP-MIi Order. We kindly request the removal of this clause to create a more inclusive environment for local suppliers. Eliminating this clause would allow local players like us to participate and contribute to the tender.	Necessary corrigendum will be issued.