# TAMIL NADU GRAMA BANK

**REF RFP No: TMD/3/2025-26 dated 28/07/2025**

## Queries and Clarifications 2

| S.No. | RFP Page No. | Clause No. | Category/Type | RFP Clause | Bidder's Query | Response/ Clarification By Bank |
|---|---|---|---|---|---|---|
| 1 | 4 | | GENERAL TENDER DETAILS - Note | "Services" means those services ancillary to the deliverables of the Company covered under the Contract. | Bidder's scope shall be limited to the items expressly set out in the proposal. Any changes to the scope shall be subject to a mutually agreed Project Change Request in writing setting out the changes in the scope and related changes in timelines, commercials, and other implications | Please adhere to the terms and conditions of RFP. |
| 2 | 8 | 3.1 | PRE-QUALIFICATION CRITERIA OF THE BIDDER (Corrigendum - Amendments - Point 105) | Subsidiary companies may use financials of the parent company for demerging entities. However, technical experience should be complied by the subsidiary company only i.e., bidding company only. | Subsidiary companies may use financials of the parent company for demerging entities. However, technical experience should be complied by the subsidiary company only i.e., bidding company only | Please refer to the amendments. |
| 3 | 8 | 6 | PRE-QUALIFICATION CRITERIA OF THE BIDDER | The Bidder should be an OEM authorized partner for atleast two years as on the date of publication of this RFP for Internal Firewall, External Firewall, WAF, EDR, SIEM, NAC and DLP solutions. The bidder should be an OEM authorized partner for all other solutions except mentioned above as on the date of publication of this RFP. The bidder should submit the manufacturer's Authorization Form for all the products/solutions quoted for this RFP. | Request to Amend-<br>The Bidder should be an OEM authorized partner for atleast two years as on the date of publication of this RFP for Internal Firewall, External Firewall, WAF, EDR, SIEM, ~~NAC~~ and DLP solutions. The bidder should be an OEM authorized partner for all other solutions except mentioned above as on the date of publication of this RFP. The bidder should submit the manufacturer's Authorization Form for all the products/solutions quoted for this RFP.<br>Since NAC is not widely adoptable technology in modern enterprise envinorment due to adoption of emerging technology like device/user authentication, ZTNA,SASE . | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | 8 | 9 | PRE-QUALIFICATION CRITERIA OF THE BIDDER | The bidder should have supplied CSOC setup comprising A) SIEM (minimum 5000 EPS) and B)(Any one of WAF/EDR/ NAC Solution) to the customer on premises, deployed the said solutions in customer's infrastructure and manage the setup on or before 31/03/2023 and continue to run as on the date of publication of RFP in at least two of the Government/banking (public or private)/financial institutions in India. The SIEM product proposed in this tender by the bidder, should be the same SIEM which was implemented earlier, for which supporting documents to be submitted. | **kindly rephrase the statement as** "The bidder should have supplied CSOC setup comprising A) SIEM (minimum 5000 EPS) and B)(Any one of WAF/EDR/ NAC Solution) to the customer on premises, deployed the said solutions in customer's infrastructure and manage the setup on or before 31/03/2024 and continue to run as on the date of publication of RFP in at least two of the Government/banking (public or private)/financial institutions in India. The OEM bidder is proposng must have atleast two references of on-premise deployment with minimum 5000 EPS in Government/banking (public or private)/financial institutions in India." | Please adhere to the terms and conditions of RFP. |
| 5 | 8 | 9 | PRE-QUALIFICATION CRITERIA OF THE BIDDER | The bidder should have supplied CSOC setup comprising A) SIEM (minimum 5000 EPS) and B)(Any one of WAF/EDR/ NAC Solution) to the customer on premises, deployed the said solutions in customer's infrastructure and manage the setup on or before 31/03/2023 and continue to run as on the date of publication of RFP in at least two of the Government/banking (public or private)/financial institutions in India. The SIEM product proposed in this tender by the bidder, should be the same SIEM which was implemented earlier, for which supporting documents to be submitted. | Request to amend the clause as The bidder should have **supplied or Managed** CSOC setup comprising A) SIEM (minimum 5000 EPS) and B)(Any one of WAF/EDR/ NAC Solution) to the customer on premises, | Please adhere to the terms and conditions of RFP. |
| 6 | 9 | 5.f | OTHER CONDITIONS | The bidder should not engage in sub-contracting during the tenure of this RFP. The bidder shall not subcontract, delegate, assign or transfer any portion of the work under this RFP to any third party without the prior written consent of the Bank. The Bank will be free to do evaluation, before accepting the third party. Any un- | Bidder should be allowed to assign its right to receive payments under the contract | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | authorized subcontracting shall constitute material breach of this RFP. | | |
| 7 | 9 | 5.f | OTHER CONDITIONS | The bidder should not engage in sub-contracting during the tenure of this RFP. The bidder shall not subcontract, delegate, assign or transfer any portion of the work under this RFP to any third party without the prior written consent of the Bank. The Bank will be free to do evaluation, before accepting the third party. Any un-authorized subcontracting shall constitute material breach of this RFP. | Considering multiple technology involved ,shorter implementation timeline and arranging bidder skilled resources (SME's) from different projects will be a challenging hence we request to consider the subcontracting during project implementation.However Bidder will be whole responsibility for meeting the project timeline and SLA requirements also bidder will get prior approval from Bank before deploying of the subcontract. | Please adhere to the terms and conditions of RFP. |
| 8 | 10 | 5.k | OTHER CONDITIONS | Out of all solutions/products in scope of work, not more than three solutions can be quoted from same OEM | There are multiple products are asked in this RFP. So bank should consider atleast four solutions to be allows from Same OEM. | Please adhere to the terms and conditions of RFP. |
| 9 | 10 | 5.k | OTHER CONDITIONS | Out of all solutions/products in scope of work, not more than three solutions can be quoted from same OEM | A single vendor cybersecurity solution offers a unified, integrated approach that simplifies management, enhances visibility, and ensures faster threat detection and response. With centralized control, consistent policy enforcement, and seamless communication between tools, it reduces complexity, lowers operational costs, and eliminates integration gaps common in multi-vendor environments. It also streamlines support with a single point of accountability, making it an efficient and secure choice for organizations looking to strengthen their cyber defense. Hence we request to remove this clause or allow positioning at least 6 products of the list. | Please adhere to the terms and conditions of RFP. |
| 10 | 10 | 5.l | OTHER CONDITIONS | Bank intends to have different OEM for internal firewall and external firewall. OEM of the SD-WAN solution running in the bank should not be proposed for internal firewall and external firewall. | The SD-WAN hub firewall is designed to manage secure and optimized WAN traffic between branches, while the DC internal and external firewalls serve entirely different purposes—protecting east-west traffic within the data center and securing north-south traffic at the perimeter, respectively. These functions are logically and operationally distinct, with no overlap or dependency, making the choice of SD-WAN OEM independent of the | Please adhere to the terms and conditions of RFP since Bank intends to adopt multi-layered defense strategy. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | internal and external firewall OEMs. Hence we request to remove this clause. | |
| 11 | 10 | 5.m | OTHER CONDITIONS | The successful bidder should provide SBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of contract. Solution should be comprehensive in nature. | SBOM is confidential related to product code, libraries and other modules and cannot be shared with any bidder.<br>Pls allow OEM to share SBOM directly to the bank after issuance of purchase order to successful bidder. | Please refer to the amendments. |
| 12 | 10 | 5.m | OTHER CONDITIONS | The successful bidder should provide SBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of contract. Solution should be comprehensive in nature. | SBOM is confidential related to product code, libraries and other modules and cannot be shared with any bidder.<br>Pls allow OEM to share SBOM directly to the bank after issuance of purchase order to successful bidder. | Please refer to the amendments. |
| 13 | 10 | 5.m | OTHER CONDITIONS | The successful bidder should provide SBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of | SBOM is confidential related to product code, libraries and other modules and cannot be shared with any bidder.<br>Pls allow OEM to share SBOM directly to the bank after issuance of purchase order to successful bidder. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | contract. Solution should be comprehensive in nature. | | |
| 14 | 10 | 5.m | OTHER CONDITIONS | The successful bidder should provide SBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of contract. Solution should be comprehensive in nature. | SBOM is confidential related to product code, libraries and other modules and cannot be shared with any bidder.<br>Pls allow OEM to share SBOM directly to the bank after issuance of purchase order to successful bidder. | Please refer to the amendments. |
| 15 | 18 | 23 | Delivery & Implementation | Bidder shall be responsible for delivery, installation, configuration, commissioning, implementation, maintenance, management and monitoring of the offered solutions, hardware and its associated components at locations specified by the Bank or any other alternate site as per the Bank's requirement. The point of delivery/ destination and site for operations will be as defined by the Bank in the Purchase Order.<br>The last date on which all the components of the solution as per Bank's Purchase Order have been delivered at the locations of the Bank, the said date will be treated as delivery date of the components. In case of delayed delivery or incorrect delivery, then date of receipt of the correct and final component shall be treated as delivery date for penalty and other calculation. Bank expects implementation by on-site resources only.<br>In case of delay on part of bidder in completion | Since Bidder is implementing the product and getting certificate from OEM is challenging and also it impacts project timeline and increase the bid cost as OEM will charge for Professional services for providing the certificates. Hence request to delete the OEM certification requirement. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | of project or initiating services will attract a penalty/termination of contract as defined in this RFP. **Upon the implementation of product/solution within the given timelines, then SI should provide certificate from O.E.M for implementation of all features required as per RFP.** | | |
| 16 | 20 | 26 | LIQUIDATED DAMAGES Deliverables: Delivery of all the Appliances/ Hardware/Appli cation Software and applicable licenses | The penalties mentioned hereunder will be applicable to the respective solutions for which the delivery/ Implementation/deployment is delayed. The penalties will be applicable even if a part of a solution/product is undelivered/unimplemented owing to which the solution/product is impacted. | We understand that LD will be applicable only on the undelivered portion/product of respective solutions.Please confirm | It is clarified that LD will be applicable for Appliances/Hardwar e/Application software and applicable licenses which are not delivered, implemented within the timelines mentioned in the RFP. |
| 17 | 25 | 29 | Insurance | The hardware/equipment to be supplied under the contract period shall be fully insured (110% of value) by the bidder till signoff between the Bank and the bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery, installation and integration. Bank will not be responsible for any loss to bidder on account of non-insurance to any equipment or services. All expenses towards insurance shall be borne by the successful bidder. | Note that under our organisational insurance policies, we are unable to disclose copies of the insurance policies and name Owner as additional insured.<br><br>This clause should be replaced with the following:<br><br>(a) The Contractor shall maintain such insurances as required by it under applicable laws of India.<br><br>(b) Upon request, the Contractor shall provide the Owner with a certificate of insurances maintained by it. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | 27 | 34 | Indemnity | The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes (except GST) and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidder's obligation under these general conditions or for which the bidder has assumed responsibilities under this contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed/ deployed/services utilized by the bidder or bidders in connection with the performance/ discharge of any system/ obligations covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to confirm and effectuate the purchase contract and to protect the Bank during the tenure of Purchase Order. Where any patent, trademark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liable for settling with such third party and paying any license fee, royalty and/ or compensation, etc., thereon. In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the solution supplied by the bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidder's cost against such third party's claim and / or actions and against any law suits of any kind initiated against the Bank. Successful bidder will also assume full responsibility of any loss and/or damages, cost, expenses, etc., caused due to malfeasance/misfeasance of any of its solution and/or due to any of their onsite engineer/representative. | We request this section to be replaced with the following:<br><br>If a third party asserts a claim against Owner that an Bidder's services acquired under the Agreement infringes a patent or copyright, Bidder will defend Owner against that claim and pay amounts finally awarded by a court against Owner or included in a settlement approved by Bidder. Owner must promptly: i) notify Bidder in writing of the claim; ii) supply information requested by Bidder; and iii) allow Bidder to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | 30 | 43 | LIMITATION OF LIABILITY | Successful Bidder's aggregate liability under the Contract shall be limited to a maximum of the Contract value. For the purposes of this clause, Contract value at any given point of time, means the aggregate value of the purchase orders, paid by Bank to the Successful Bidder that gives rise to claim, under this Contract. In the following circumstances limitation of liability shall not apply and the Successful Bidder shall be liable for amount of cost, damages, compensation, penalty etc. suffered by the Bank:<br><br>a) Liability of Successful Bidder for third party claims for IP Infringement.<br>b) Liability of Successful Bidder (including third party claims) in case of bodily injury (including Death).<br>c) Liability of Successful Bidder (including third party claims) in case of damage to real property and tangible property caused by the bidder's gross negligence.<br>d) Liability of the Successful Bidder in case of gross negligence or willful misconduct attributable to the Successful Bidder while providing services under this Contract.<br>e) Liability of the Successful Bidder in case of fraudulent acts or willful misrepresentation attributable to the Vendor regarding the services provided under this Contract.<br>f) Breach of the confidentiality.<br>g) Employment liabilities for Successful Bidder's staff relating to the period of their employment within contractual period while working with Bank.<br>h) Any liability/penalty/cost/compensation/charges etc. that cannot be capped or is excluded as a matter of applicable laws and imposed by the statutory authority/ government bodies/ court/tribunals etc. in relation to this Contract, owing to the fault of the Successful Bidder. | We request the following to be clarified in the contract:<br><br>Bidder's entire liability for all claims related to the contract will not exceed the amount of any actual direct damages incurred by Owner up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim. Bidder will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 20 | 31 | 44 | DISPUTE RESOLUTION /ARBITRATION | All disputes or differences whatsoever arising between the parties out of or in relation to the construction, meaning and operation or effect of the said Contract or breach thereof shall be settled amicably. If, however, the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996, the matter may be referred to a sole arbitrator who may be appointed mutually by both the Parties and the award made in pursuance thereof shall be binding on the parties. The venue of the arbitration shall be Chennai. The Arbitrator/Arbitrators shall give a reasoned award. Any appeal will be subject to the exclusive jurisdiction of courts at Chennai. Successful Bidder Shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the approval of bank in writing that the events are such where work cannot possibly be continued or until the decision to the contrary of the arbitrator or the umpire, as the case may be, has been obtained by Successful bidder. However, during such a contingency, the Bank shall be entitled to make alternative arrangements in any manner it deems fit, at the cost of the Successful bidder which may also be adjusted by the Bank from the Performance Bank Guarantee, being treated as default so that the business of the Bank is not disrupted. Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal/ other legal recourse. | We request this section to be replaced with the following:<br><br>Both parties agree to the application of the laws of India , without regard to conflict of law principles. Disputes shall be finally settled in accordance with The Arbitration and Conciliation Act, 1996 then in effect, in English, with seat in Bangalore, India. There shall be one arbitrator if the amount in dispute is less than or equal to Indian Rupee five crores and three arbitrators if the amount is more | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 21 | 33 | 1.2 | SCOPE OF WORK - External Firewall | The new firewall solution should comprise of Firewall rule analyser feature, Anti APT, Sandboxing and NIPS. | Requesting bank to separate the Sandbox from Firewall.<br><br>**Justification:** With respect to firewall, it has a dedicated work to filter out the good traffic from huge amount of bad traffic. For this activity it needs good amount of processing speed. Enabling multiple other features in the same Appliance may degraded the overall performance. The purpose of Sandbox is also to find out the unknown threats which needs huge processing power and analysis time. Adding these technologies with Firewall is not a proper ask.<br><br>As per the best practice and adherence to defence in depth architecture, every critical infrastructure should consider dedicated purpose-built solutions for each of these activities.<br>**Referring to the Indian bank architecture, TNGB should consider a separate Sandboxing for Endpoints/Servers. Indian bank is already using AV , EDR and Sandbox from same Vendor.** | Please adhere to the terms and conditions of RFP. |
| 22 | 33 | 1.2 | SCOPE OF WORK - External Firewall | The new firewall solution should comprise of Firewall rule analyser feature, Anti APT, Sandboxing and NIPS. | Requesting bank to separate the Sandbox from Firewall.<br><br>**Justification:** With respect to firewall, it has a dedicated work to filter out the good traffic from huge amount of bad traffic. For this activity it needs good amount of processing speed. Enabling multiple other features in the same Appliance may degraded the overall performance. The purpose of Sandbox is also to find out the unknown threats which needs huge processing power and analysis time. Adding these technologies with Firewall is not a proper ask.<br><br>As per the best practice and adherence to defence in depth architecture, every critical infrastructure should | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | consider dedicated purpose-built solutions for each of these activities.<br>**Referring to the Indian bank architecture, TNGB should consider a separate Sandboxing for Endpoints/Servers. Indian bank is already using AV , EDR and Sandbox from same Vendor.** | |
| 23 | 33 | 1.2 | SCOPE OF WORK - External Firewall | The new firewall solution should comprise of Firewall rule analyser feature, Anti APT, Sandboxing and NIPS. | Requesting bank to separate the Sandbox from Firewall.<br><br>**Justification:** With respect to firewall, it has a dedicated work to filter out the good traffic from huge amount of bad traffic. For this activity it needs good amount of processing speed. Enabling multiple other features in the same Appliance may degraded the overall performance. The purpose of Sandbox is also to find out the unknown threats which needs huge processing power and analysis time. Adding these technologies with Firewall is not a proper ask.<br><br>As per the best practice and adherence to defence in depth architecture, every critical infrastructure should consider dedicated purpose-built solutions for each of these activities.<br>**Referring to the Indian bank architecture, TNGB should consider a separate Sandboxing for Endpoints/Servers. Indian bank is already using AV , EDR and Sandbox from same Vendor.** | Please adhere to the terms and conditions of RFP. |
| 24 | 33 | 1.3 | SCOPE OF WORK - Centralized Log Management Solution (CLMS) | Bidder to provide 200 licenses for log management solution. | Bank mentioned on 200 log sources. Need to know the EPS count or share the device list to calculate the EPS | It is clarified that Bank intends to collect and store logs from Servers, iPDUs, Storage, Applications, Databases, Network devices and all other |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | security solutions proposed in this RFP. |
| 25 | 33 | 1.3 | SCOPE OF WORK - Centralized Log Management Solution (CLMS) / Corrigendum - Page 63 Point 142 | **RFP Clause:** • Bidder to provide 200 licenses for log management solution. • DC and DR setup for the solution to be implemented without HA. • However the log sources may be at various locations as required by bank. **Corrigendum Clause:** Yes. SIEM OEM may be considered for CLMS provided all the technical specifications are met. | Bank's response mentiones that SIEM and CLMS to be separate solutions, whereas in page 63, point 142, it mentions SIEM OEM may be considered for CLMS. Please clarify. | It is clarified that if a product from an OEM meets all the technical specifications of SIEM and CLMS mentioned in this RFP, the same can be quoted. In that case, bank will consider 2 solutions are proposed from the same OEM. |
| 26 | 35 | 1.y | SCOPE OF WORK | All the solutions have to be integrated in SIEM as well as in CLMS/Syslog servers for necessary system logs before Signing-Off the respective solutions. The Bank will verify that the proper log details are being received by the SIEM and CLMS/Syslog Server or not. | Request bank to have SIEM and CLMS as a apart of same SIEM solution instead of having two different solution. | It is clarified that if a product from an OEM meets all the technical specifications of SIEM and CLMS mentioned in this RFP, the same can be quoted. In that case, bank will consider 2 solutions are proposed from the same OEM. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 27 | 39 | 4 | INDIVIDUAL ROLE & RESPONSIBILITIES OF ONSITE, OFFSITE AND ONCALL TECHNICAL SUPPORT RESOURCES : **Level 2 Onsite Support** | **Corrigendum Clause:**<br>b) Deployment and Installation of all in scope solutions and their monitoring<br>c) Upgradation of all in scope solutions and their monitoring<br>d) Configuration and management of cyber security solutions/ components under the scope.<br>e) Deployment of all in scope solutions | We understand while all applications will be installed and deployed through patch management and asset management solution, kinly clarify whether bank as any tools to install the patch management software first time across the devices mentioned. | It is clarified that Bank had implemented Microsoft AD and the same may be leveraged for implementation of Patch management solution. |
| 28 | 43 | 6 | DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS: ( DC and DR implementation should be done in parallel.) | Delivery of Hardware/ Appliance/ Licenses at respective locations ( Sr No 1 to 15)-Within 8 weeks from date of PO Acceptance | Delivery of IT Hardware like server ,storage,san switches etc will take delivery lead time of 12 weeks hence we request to Amend the clause as below-<br><br>Delivery of Hardware/ Appliance/ Licenses at respective locations ( Sr No 1 to 15)-Within ~~8~~ 12 weeks from date of PO Acceptance. | Please adhere to the terms and conditions of RFP. |
| 29 | 43 | 6 | DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS: ( DC and DR implementation should be done in parallel.) | Implementation/ Integration/GoLive/ Sign-Off at respective locations | Considering various bank branches across the state, rollout of EDR,DLP,NAC within 16 to 18 weeks is challenging and also bidder needs to keep the IT infra ready for the above roll out.Hence we request to amend the clause as below-<br><br>DC/ DR components deployment - 16 weeks from date of PO<br>Patch Management Roll out and EDR,DLP ,NAC agent rollout across branches -30 weeks from date of PO | Please adhere to the terms and conditions of RFP. |
| 30 | 45 | 1.13 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS | The Firewall solution should support Role-based administrative access and also MFA for the same | **Request to update clause as :** The Firewall solution should have Role-based administrative access and should be able to integrate with MFA. **Justification:** MFA is not the native functionality of thr | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | -INTERNAL FIREWALL | | firewall, however it can be intergated with MFA for 2 factor authentication | |
| 31 | 45 | 1.13 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should support Role-based administrative access and also MFA for the same | The Firewall solution should have Role-based administrative access and should be able to integrate with MFA | Please refer to the amendments. |
| 32 | 46 | 1.15 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should support import and export of security policies (in .csv and .xls files) \configurations without any downtime | **Request to update clause as:** The Firewall solution should be able to import and export of security policies/configurations through API without any downtime. **Justification:** Every OEM has own way for achieving this requirment. | Please refer to the amendments. |
| 33 | 46 | 1.15 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should support import and export of security policies (in .csv and .xls files) \configurations without any downtime | The Firewall solution should be able to import and export of security policies/configurations through API without any downtime | Please refer to the amendments. |
| 34 | 46 | 1.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The supported number of concurrent sessions should be minimum 1000000 | **Request to update clause as:** Must support at least 1000000 L3 concurrent session OR New Layer 7/app-id/AVC connections per second – Min 6 million. **Justification:** The ask feature set are of NGFW . NGFW differentiate from its predecessor that rules are define with application (micro/macro) instead of ports and hence it is important the connections and connections per second should be with L7/AVC paramters for correct sizing. | Please adhere to the terms and conditions of RFP. |
| 35 | 46 | 1.21 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The other physical ports should be- at least 4 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 8 nos. of 10G SFP+- | **Request to update clause as:** The other physical ports should be- 8 x 1/10 Gig interfaces and 2 x 40G interfaces. **Justification:** 1G copper interfaces are obsolete in enterprice firewall, the Firewall need to integrate with existing Cisco border leaf with minimum 40G as 10G connection will be a bottle neck and will create performance impact on the east west traffic. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 36 | 46 | 1.21 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The other physical ports should be- at least 4 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 8 nos. of 10G SFP+- | The other physical ports should be- 8 x 1/10 Gig interfaces and 2 x 40G interfaces | Please adhere to the terms and conditions of RFP. |
| 37 | 46 | 1.18 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The supported number of new connections per second should be minimum 300000 | **Request to update clause as:** Must support at least 300000 L3 new sessions per second processing OR New Layer 7/app-id/AVC connections per second – Min 230,000. **Justification:** The ask feature set are of NGFW . NGFW differentiate from its predecessor that rules are define with application (micro/macro) instead of ports and hence it is important the connections and connections per second should be with L7/AVC paramters for correct sizing. | Please adhere to the terms and conditions of RFP. |
| 38 | 47 | 1.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The supported number of concurrent sessions should be minimum 1000000 | Must support at least 1000000 L3 concurrent session OR New Layer 7/app-id/AVC connections per second – Min 6 million | Please adhere to the terms and conditions of RFP. |
| 39 | 47 | 1.36 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should provide insights on unused rule\policy and provide optimization recommendations | **Request to update clause as:** The Firewall solution should provide insights on unused rule\policy. **Justification:** Policy optimization recommendations can be achieved with cloud delivered FMC, which requires cloud management. | Please adhere to the terms and conditions of RFP. |
| 40 | 47 | 1.36 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should provide insights on unused rule\policy and provide optimization recommendations | The Firewall solution should provide insights on unused rule\policy. | Please adhere to the terms and conditions of RFP. |
| 41 | 47 | 1.18 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The supported number of new connections per second should be minimum 300000 | Must support at least 300000 L3 new sessions per second processing OR New Layer 7/app-id/AVC connections per second – Min 230,000 | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 42 | 48 | 1.53 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | Appliance must have minimum 128 GB of RAM and 240 GB storage | Fortinet uses custom Application-Specific Integrated Circuits (ASICs), like the NP (Network Processor) and CP (Content Processor) ASICS. These ASICS offload and accelerate specific tasks such as:<br><br>Fast path traffic forwarding (NP)<br>Content inspection, SSL decryption (CP)<br>IPsec VPN encryption/decryption<br><br>This hardware acceleration reduces CPU load and enhances throughput. The RAM on any hardware functions to hold session table, route table,etc and is optimally sized individually by every OEM for performance numbers in the datasheet for the respective hardware. Hence, FortiGates can offer the throughput specified on the Datasheet with the RAM available in the system. Hence we request you to remove this clause as this specification will not improve performance. | Please adhere to the terms and conditions of RFP. |
| 43 | 55 | 3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM, Corrigendum | **Additional clause-General Points Corrigendum Clause: (412)** It is clarified that SIEM is to be implemented in Active-Passive architecture. | HA within site for SIEM has been asked, whereas in page 128, point 412, it mentions as Active-Passive architecture, please clarify if HA at DC is required? | It is clarified that SIEM is to be configured in Active-Passive mode within a site to ensure HA. |
| 44 | 55 | 3.6 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The solution must support identification (automated/manual) and classification for type of assets (i.e. servers, network devices, mail servers, data base servers, etc.,). The solution should be able to accept and integrate with asset details to provide asset level events, incidents, vulnerabilities, and issues. | We understand that the bank is expecting to integrate SIEM solution with the vulnerability management which allows to integrate data that can be retrieved from VA vendors and showcase the known vulnerability details via threat intelligence or via TIP platform. Please confirm if the understanding is inline with the bank expectations. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 45 | 57 | 3.20. | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The system should support, not restricted to, the following log and event collection methods:· Syslog – UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195)· Flat file logs such as from DNS, DHCP, Mail servers, web servers etc.· Windows events logs – Agent-based or agentless· FTP, S/FTP, SNMP, SCP,ODBC, CP-LEA, SDEE, WMI,JDBC,AIX,SAP, single and multi-line flat files,API,Netflow etc. | Request to amend this clause as below: "The system should support, not restricted to, the following log and event collection methods:· Syslog – UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195), Native log integration, Windows events logs – Agent-based or agentless· FTP, S/FTP, SNMP, SCP, API, NetFlow etc." | Please adhere to the terms and conditions of RFP. |
| 46 | 58 | 3.42 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The Proposed solution should be capable to detect Slow attacks, advance persistent threats, file less attacks, advance malwares, zero -day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI or ML or both. Also, capable to prevent & predict known- known, knownunknown and unknown-unknown<br>threats by monitoring entire IT infrastructure and leveraging real time threat intelligence | There are multiple ways/techniques to detect " *detect Slow attacks, advance persistent threats, file less attacks, advance malwares, zero -day attacks, in-memory attacks"* not all attacks are covered via *"in-built self-learning and analytics leveraging AI or ML or both"* only e.g.,<br><br>1. Zero days attacks are detected via TI feed, Integration with IPS/IDS, SYSMON etc.<br>2. advance malwares are detected via C2C detection (TI), Sandbox solution integration, SYSMON/EDR logs etc.<br><br>please change this clause to *"The Proposed solution should be capable to detect Slow attacks, advance persistent threats, file less attacks, advance malwares, zero -day attacks, in-memory attacks, leveraging AI or ML/Integrations/TI feed/Correlation or any similar detection techniques . Also, capable to prevent & predict known- known, knownunknown and unknown-unknown threats by monitoring entire IT infrastructure and leveraging real time threat intelligence"* | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 47 | 59 | 3.56 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier. | Point 59 and 80 both are indicating towards NTA/NBAD/packet Capture, but in clause 80 it is mentioned that "*Bidder does not require to provide NTA and NBAD in this bid*". Please clarify that both points "56 and 80" are only applicable if Bank provides current deployed NTA or in future. " Request to remove the clause" | Please refer to the amendments. |
| 48 | 59 | 3.6 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The solution should be capable to store 3 Months data online on storage device and able to archive one year data from **Syslog server provided by the bank.** | We understand that back is expecting to store the raw logs on the CLMS and selected security incidents to the SIEM solution with different storage retention. Please confirm if the understanding is in line with the bank expectations. | Your understanding is correct. |
| 49 | 75 | 5.111 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - WEB PROXY SOLUTION, Corrigendum | Even if the solution are functioning in active-passive mode all the reports and logs should be available in the central console. | HA within site for Web Proxy has been asked, whereas the RFP ask is Active-Passive mode. Please clarify | It is clarified that Bank intends to have web proxy configured in Active-Passive mode ensuring HA. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 50 | 78 | 6.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - CLMS, Corrigendum | **RFP Clause:** The retention duration should be flexible ( current requirement is 5 years for VPN logs and 1 year for other logs). **Corrigendum Clause:** (469) Please adhere to the terms and conditions of RFP. **RFP Clause :** • Bidder to provide 200 licenses for log management solution. • DC and DR setup for the solution to be implemented without HA. • However the log sources may be at various locations as required by bank **Corrigendum Clause:** It is a Greenfield Implementation and device details will be shared with successful bidder. The rolling log retention period for CLMS is as follows online: 270 days offline: Bank will provide tape back up infrastructure. | For the CLMS query raised on point which mentions 5k EPS for VPN logs, the corrigendum mentions to adhere to the RFP terms. Whereas, in page number 63, point 143, the revised clause mentions as 270 days of online logs. Please clarify which one to consider. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 51 | 82 | 7.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux .<br><br>**Amended Clause**: "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Requesting bank to modify clause as follows "**The proposed solution must support Microsoft Windows client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. If you are considering Linux machines for any other purpose for branch offices kindly share the quantity and also include in the Price bid under HIPS.<br><br>**Justification:** With respect to server security for Linux Environment, Trend Micro is proposing a purpose-built solution, Deep Security that has multiple modules which go beyond Antimalware. Modules like Virtual patching provide protection against vulnerabilities and virtually shield it until OEM patches are applied. Furthermore, modules like Integrity Monitoring and Log Inspection, deep dive into the server level and help track changes done to critical files, folders, registries, processes. (Which can indicate an impending attack). Log inspection module inspects OS and application-level logs and highlight the ones that indicate suspicious activity. Alerts generated from these modules are mapped to MITRE ATT&CK framework which helps organization track the TTPs that are being used inside the system. Application control helps to blacklisting bad IOCs that need to be blocked for preventing malicious application execution or any unauthorized application and help to harden the server. All these modules put together drastically reduce the attack surface and provide insights that can help detect attack at an early stage and remediate it subsequently. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 52 | 82 | 7.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux .<br><br>**Amended Clause**: "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Requesting bank to modify clause as follows "**The proposed solution must support Microsoft Windows client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. If you are considering Linux machines for any other purpose for branch offices kindly share the quantity and also include in the Price bid under HIPS.<br><br>**Justification:** With respect to server security for Linux Environment, Trend Micro is proposing a purpose-built solution, Deep Security that has multiple modules which go beyond Antimalware. Modules like Virtual patching provide protection against vulnerabilities and virtually shield it until OEM patches are applied. Furthermore, modules like Integrity Monitoring and Log Inspection, deep dive into the server level and help track changes done to critical files, folders, registries, processes. (Which can indicate an impending attack). Log inspection module inspects OS and application-level logs and highlight the ones that indicate suspicious activity. Alerts generated from these modules are mapped to MITRE ATT&CK framework which helps organization track the TTPs that are being used inside the system. Application control helps to blacklisting bad IOCs that need to be blocked for preventing malicious application execution or any unauthorized application and help to harden the server. All these modules put together drastically reduce the attack surface and provide insights that can help detect attack at an early stage and remediate it subsequently. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 53 | 82 | 7.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux .<br><br>**Amended Clause**: "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Requesting bank to modify clause as follows "**The proposed solution must support Microsoft Windows client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. If you are considering Linux machines for any other purpose for branch offices kindly share the quantity and also include in the Price bid under HIPS.<br><br>**Justification:** With respect to server security for Linux Environment, Trend Micro is proposing a purpose-built solution, Deep Security that has multiple modules which go beyond Antimalware. Modules like Virtual patching provide protection against vulnerabilities and virtually shield it until OEM patches are applied. Furthermore, modules like Integrity Monitoring and Log Inspection, deep dive into the server level and help track changes done to critical files, folders, registries, processes. (Which can indicate an impending attack). Log inspection module inspects OS and application-level logs and highlight the ones that indicate suspicious activity. Alerts generated from these modules are mapped to MITRE ATT&CK framework which helps organization track the TTPs that are being used inside the system. Application control helps to blacklisting bad IOCs that need to be blocked for preventing malicious application execution or any unauthorized application and help to harden the server. All these modules put together drastically reduce the attack surface and provide insights that can help detect attack at an early stage and remediate it subsequently. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 54 | 82 | 7.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux .<br><br>**Amended Clause**: "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Requesting bank to modify clause as follows "**The proposed solution must support Microsoft Windows client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. If you are considering Linux machines for any other purpose for branch offices kindly share the quantity and also include in the Price bid under HIPS.<br><br>**Justification:** With respect to server security for Linux Environment, Trend Micro is proposing a purpose-built solution, Deep Security that has multiple modules which go beyond Antimalware. Modules like Virtual patching provide protection against vulnerabilities and virtually shield it until OEM patches are applied. Furthermore, modules like Integrity Monitoring and Log Inspection, deep dive into the server level and help track changes done to critical files, folders, registries, processes. (Which can indicate an impending attack). Log inspection module inspects OS and application-level logs and highlight the ones that indicate suspicious activity. Alerts generated from these modules are mapped to MITRE ATT&CK framework which helps organization track the TTPs that are being used inside the system. Application control helps to blacklisting bad IOCs that need to be blocked for preventing malicious application execution or any unauthorized application and help to harden the server. All these modules put together drastically reduce the attack surface and provide insights that can help detect attack at an early stage and remediate it subsequently. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 55 | 85 | 1.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | The proposed solution should be able to support Windows, MAC, Ubuntu and Linux (all flavours like Oracle, RHEL etc) operating systems.<br><br>**Amended Clause:** "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Request bank to modify the clause as follows "**The proposed solution must support Microsoft Windows and MAC client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. | Please refer to the amendments. |
| 56 | 85 | 1.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | The proposed solution should be able to support Windows, MAC, Ubuntu and Linux (all flavours like Oracle, RHEL etc) operating systems.<br><br>**Amended Clause:** "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Request bank to modify the clause as follows "**The proposed solution must support Microsoft Windows and MAC client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 85 | 1.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | The proposed solution should be able to support Windows, MAC, Ubuntu and Linux (all flavours like Oracle, RHEL etc) operating systems.<br><br>**Amended Clause:** "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Request bank to modify the clause as follows "**The proposed solution must support Microsoft Windows and MAC client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. | Please refer to the amendments. |
| 58 | 85 | 1.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | The proposed solution should be able to support Windows, MAC, Ubuntu and Linux (all flavours like Oracle, RHEL etc) operating systems.<br><br>**Amended Clause:** "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | Request bank to modify the clause as follows "**The proposed solution must support Microsoft Windows and MAC client operating system**."<br><br>**Justification:**<br>AV and EDR are basically used to protect User Endpoints such as Windows Laptops and Desktops variants.<br><br>Server platform which is running on Windows and Linux Flavours (RHEL, Cent OS, Ubuntu, SUSE, Oracle Linux etc.), there is a separate Server Security component which is already asked in the same RFP as part of HIPS requirement. | Please refer to the amendments. |
| 59 | 85 | 7.2.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. | Request bank to modify this clause as follows "**Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. The restart maybe required for critical or exceptional cases**" | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 60 | 85 | 7.2.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. | Request bank to modify this clause as follows "**Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. The restart maybe required for critical or exceptional cases**" | Please refer to the amendments. |
| 61 | 85 | 7.2.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. | Request bank to modify this clause as follows "**Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. The restart maybe required for critical or exceptional cases**" | Please refer to the amendments. |
| 62 | 85 | 7.2.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. | Request bank to modify this clause as follows "**Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. The restart maybe required for critical or exceptional cases**" | Please refer to the amendments. |
| 63 | 88 | 7.2.45 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | 2.45 The proposed solution should have the option to block the intruder hosts for a specific number of seconds.<br><br>**Amended Clause:** "The proposed solution should have the option to block/isolate/quarantine the intruder hosts for a specific number of seconds." | Requesting bank to modify the clause as follows "**The proposed solution must block/isolate/quarantine affected host during malicious activity**."<br><br>**Justification:** If an asset is affected then it must be blocked/isolated/quarantine until it gets cleared. It does not make sense to act only for a specific period. Because once the specified time is reached the endpoint will start communicating with other devices and spreading the malware to other endpoint devices. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 64 | 88 | 7.2.45 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | 2.45 The proposed solution should have the option to block the intruder hosts for a specific number of seconds.<br><br>**Amended Clause:** "The proposed solution should have the option to block/isolate/quarantine the intruder hosts for a specific number of seconds." | Requesting bank to modify the clause as follows "**The proposed solution must block/isolate/quarantine affected host during malicious activity**."<br><br>**Justification:** If an asset is affected then it must be blocked/isolated/quarantine until it gets cleared. It does not make sense to act only for a specific period. Because once the specified time is reached the endpoint will start communicating with other devices and spreading the malware to other endpoint devices. | Please refer to the amendments. |
| 65 | 88 | 7.2.45 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | 2.45 The proposed solution should have the option to block the intruder hosts for a specific number of seconds.<br><br>**Amended Clause:** "The proposed solution should have the option to block/isolate/quarantine the intruder hosts for a specific number of seconds." | Requesting bank to modify the clause as follows "**The proposed solution must block/isolate/quarantine affected host during malicious activity**."<br><br>**Justification:** If an asset is affected then it must be blocked/isolated/quarantine until it gets cleared. It does not make sense to act only for a specific period. Because once the specified time is reached the endpoint will start communicating with other devices and spreading the malware to other endpoint devices. | Please refer to the amendments. |
| 66 | 88 | 7.2.45 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | 2.45 The proposed solution should have the option to block the intruder hosts for a specific number of seconds.<br><br>**Amended Clause:** "The proposed solution should have the option to block/isolate/quarantine the intruder hosts for a specific number of seconds." | Requesting bank to modify the clause as follows "**The proposed solution must block/isolate/quarantine affected host during malicious activity**."<br><br>**Justification:** If an asset is affected then it must be blocked/isolated/quarantine until it gets cleared. It does not make sense to act only for a specific period. Because once the specified time is reached the endpoint will start communicating with other devices and spreading the malware to other endpoint devices. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 67 | 89 | 4.8 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | 4.8 Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | Request you to kindly amend this clause as follows **"Solution should have the capability of allowing only whitelisted applications to run and prevent execution of any application which is tampered."**<br><br>**Justification:** OEM for Application whitelisting can prevent any tampered component of the application from running/loading in a High Enforcement scenario where no new .exe/file/script etc can be executed. That is the essence of a whitelisting does not allow any new file/exe or script to get executed and adhere to zero trust model, only allow/trusted apps to run and anything else either good or bad to be blocked, with exclusion for tools like patch management/publishers etc. | Please refer to the amendments. |
| 68 | 89 | 4.8 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | 4.8 Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | Request you to kindly amend this clause as follows **"Solution should have the capability of allowing only whitelisted applications to run and prevent execution of any application which is tampered."**<br><br>**Justification:** OEM for Application whitelisting can prevent any tampered component of the application from running/loading in a High Enforcement scenario where no new .exe/file/script etc can be executed. That is the essence of a whitelisting does not allow any new file/exe or script to get executed and adhere to zero trust model, only allow/trusted apps to run and anything else either good or bad to be blocked, with exclusion for tools like patch management/publishers etc. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 69 | 89 | 4.8 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | 4.8 Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | Request you to kindly amend this clause as follows **"Solution should have the capability of allowing only whitelisted applications to run and prevent execution of any application which is tampered."**<br><br>**Justification:** OEM for Application whitelisting can prevent any tampered component of the application from running/loading in a High Enforcement scenario where no new .exe/file/script etc can be executed. That is the essence of a whitelisting does not allow any new file/exe or script to get executed and adhere to zero trust model, only allow/trusted apps to run and anything else either good or bad to be blocked, with exclusion for tools like patch management/publishers etc. | Please refer to the amendments. |
| 70 | 89 | 4.8 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | 4.8 Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | Request you to kindly amend this clause as follows **"Solution should have the capability of allowing only whitelisted applications to run and prevent execution of any application which is tampered."**<br><br>**Justification:** OEM for Application whitelisting can prevent any tampered component of the application from running/loading in a High Enforcement scenario where no new .exe/file/script etc can be executed. That is the essence of a whitelisting does not allow any new file/exe or script to get executed and adhere to zero trust model, only allow/trusted apps to run and anything else either good or bad to be blocked, with exclusion for tools like patch management/publishers etc. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 71 | 105 | 11.2.12 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, all service running, all process running, all application version, all application installed etc. to achieve 100% device visibility with NAC. | FortiNAC does not support to give visibility on all running services and process. Fortinac can check the services and process as a posture assessment and share you the result of the passed and failed services and process which is mentioned in the posture check list. Reqeust to rephrase the statement as " Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, all service running, all process running, all application version, all application installed etc. to achieve 100% device visibility with NAC." | Please refer to the amendments. |
| 72 | 105 | 11.2.15 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The solution should provide out of the box visibility to Virtual machine properties such as Boot Time, Virtual Machine Hardware, is Virtual Machine orphan, Virtual Machine Peripheral Devices info, Virtual Machine port group, Virtual Machine power state, Virtual Machine CPU usage, Virtual Machine usage network I/O (KBPS) etc | This is a feature of SIEM and its convered as part of the CSOC solution offering. Hence we reqeust to remove this RFP specification. | Please adhere to the terms and conditions of RFP. |
| 73 | 105 | 11.2.6 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Works via agent-less, persistent client-based agent and a dissolvable/temporary agent to validate that an endpoint is conforming to a company's posture policies which includes but not limited to checks for the latest OS patches, antivirus/EDR and antispyware software packages with current definition version, Windows registries key, Windows registry value, Linux process etc., and applications, local firewalls, P2P applications, Disk Encryptions, USB Check, etc. | FortiNAC supports Registry key and Registry version only. Request rephrase of the statemenet as "Works via agent-less, persistent client-based agent and a dissolvable/temporary agent to validate that an endpoint is conforming to a company's posture policies which includes but not limited to checks for the latest OS patches, antivirus/EDR and antispyware software packages with current definition version, Linux process etc., and applications, local firewalls, P2P applications, Disk Encryptions, USB Check, etc." | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 74 | 107 | 11.5.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must be able to provide compliance for Hardware properties on windows like Hardware Computer, Disks, Display Unit, Motherboard, Network Adapter, Physical Memory, Plug and Play Device, Processor, etc. | Request to remove this specification as this is vendor specific feature. | Please refer to the amendments. |
| 75 | 107 | 11.5.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must automate the inventorying of IP-connected assets across extended enterprise networks along with detailed information of hardware viz. Disks, Display Units, Motherboard, Network Adapter, Physical Memory, Plug and Play Device, Processor, etc continuously and accurately for all connected devices. | This is a feature of SIEM and its convered as part of the CSOC solution offering. Hence we reqeust to remove this RFP specification. | Please refer to the amendments. |
| 76 | 108 | 11.6.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must support capability to generate report for hardware (Memory, RAM, HDD, Peripheral devices, etc.), all installed software with version, Open ports (TCP/UDP), Service Running, Process Running and application inventory across managed extended enterprise. | Request to remove this specification as this is vendor specific feature. | Please refer to the amendments. |
| 77 | 111 | 12.42 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -DAM | The Proposed Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats. | Kindly rephrase to “The Proposed Solution should support automatic updates to its vulnerability assessment, and provide integration with global threat intelligence sources (directly or via SIEM) to ensure protection against emerging database-related threats.”<br><br>The Guardium Vulnerability Assessment feature includes a database protection knowledge base subscription, which enables automatic updates from the Guardium Vulnerability Assessment development and research team. This ensures the system stays current with the latest vulnerabilities and test signatures. | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 78 | 112 | 13.20. | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should display icons over files that have been classified using the solution. | * This Specification / display icon over the files help to identify which are the file got classified which are the files are not classified for better classification visibility . Moreover, this is the legacy approach.<br><br>* But using proposed solution can classify the file / data-in-use using Agent & Also we can discover and classify data's-at-rest from the endpoints, Servers & Cloud repositories without agent. Ideally no files will need to leave without classification using proposed Solution. * As Display Icon overlay is the OEM Specific capabilities, Request to remove the Spec for wider participation. | Please refer to the amendments. |
| 79 | 112 | 13.20. | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should display icons over files that have been classified using the solution. | This Specification / display icon over the files help to identify which are the file got classified which are the files are not classified for better classification visibility . Moreover, this is the legacy approach. Request you to remove this clause-<br>* But using proposed solution can classify the file / data-in-use using Agent & Also we can discover and classify data's-at-rest from the endpoints, Servers & Cloud repositories without agent. Ideally no files will need to leave without classification using proposed Solution. | Please refer to the amendments. |
| 80 | 112 | 13.20. | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should display icons over files that have been classified using the solution. | * This Specification / display icon over the files help to identify which are the file got classified which are the files are not classified for better classification visibility . Moreover, this is the legacy approach.<br>* But using proposed solution can classify the file / data-in-use using Agent & Also we can discover and classify data's-at-rest from the endpoints, Servers & Cloud repositories without agent. Ideally no files will need to leave without classification using proposed Solution. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | * As Display Icon overlay is the OEM Specific capabilities, Request to remove the Spec for wider participation. | |
| 81 | 113 | 13.27 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy. | * The purpose of the tooltips is to enhance user understanding of each label to select the right labels manually. Which is also the legacy approach.<br>* With the proposed solution we have better way to educate the user with the content-based inspection wide the AI Mesh technology for effective / appropriate Label suggestions for the Users. Users simply follow the AI Suggestions which is 85%-90% accurate than the manual classification.<br>* Similar to tooltips wide the proposed solution users can use the Help link we provide to see a webpage describing all the classification labels<br>* As Tooltip is the OEM Specific terminology Request to modifying the spec as " The solution should provide tooltips or equal function, classification descriptions / help page links to assist users with classification policy" | Please refer to the amendments. |
| 82 | 113 | 13.27 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy. | The purpose of the tooltips is to enhance user understanding of each label to select the right labels manually. Which is also the legacy approach.<br>* With the proposed solution we have better way to educate the user with the content-based inspection wide the AI Mesh technology for effective / appropriate Label suggestions for the Users. Users simply follow the AI Suggestions which is 85%-90% accurate than the manual classification.<br>* Similar to tooltips wide the proposed solution users can use the Help link we provide to see a webpage describing all the classification labels | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | * As Tooltip is the OEM Specific terminology Request to modifying the spec as " The solution should provide tooltips or equal function, classification descriptions / help page links to assist users with classification policy" | |
| 83 | 113 | 13.27 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy. | * The purpose of the tooltips is to enhance user understanding of each label to select the right labels manually. Which is also the legacy approach.<br>* With the proposed solution we have better way to educate the user with the content-based inspection wide the AI Mesh technology for effective / appropriate Label suggestions for the Users. Users simply follow the AI Suggestions which is 85%-90% accurate than the manual classification.<br>* Similar to tooltips wide the proposed solution users can use the Help link we provide to see a webpage describing all the classification labels<br>* As Tooltip is the OEM Specific terminology Request to modifying the spec as " The solution should provide tooltips or equal function, classification descriptions / help page links to assist users with classification policy" | Please refer to the amendments. |
| 84 | 138 | 16 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Hosting Infrastructure, Corrigendum | **Amended Clause:** "The proposed Hardware family and Software generation should be latest from the date of RFP submission and the proposed Hardware family" | Since Intel 6th Generation is not available to quote as per Make in India Mandate, Request Bank to consider current Intel 5th Generation Processors with Make in India local content for participation | Please adhere to the terms and conditions of RFP. |
| 85 | 141 | 10 | General Requirements | **Amended Clause:** All the devices/products/solutions proposed for this RFP should not be announced End of Life, End of Service Life for seven years from the date of submission of this RFP | Herewith requesting Bank to amend as below All the devices/Hardware Family /products/solutions proposed for this RFP should not be announced End of Sale for 6 months from the date of the submission of the RFP and should be under Standard OEM Support for 7 years from the date of the submission of the RFP | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 86 | 141 | 16.6 | General Requirements, Corrigendum | **RFP Clause:** General requirements:Space for one rack of 800 mm width and 1200 mm depth will be provided by BANK in DC and DR **Amended Clause:** It is clarified that rack space for devices like firewalls, WAF, NTP will be provided by the Bank at its DC and DRS. It is expected all other solutions proposed in this RFP has to be provisioned in a single 42U rack with power limit of 4 KW at DC; for DRS bank will provide one rack. | We understand that power will exceed the 4 KW power for single 42 RU Rack, so please provision additional power in case it is needed for DC and DR Sites. | It is clarified that bank will arrange for power based upon feasibility at DC and DR sites. |
| 87 | 141 | 16.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Hosting Infrastructure - Server - Warranty | 5 Years 24/7 Warranty with 30 minutes Response Time and 4 hours Call to Resolution including part replacement, access to OEM support portal, OEM technical support on 24X7X365 basis. Successful Bidder must provide documentary proof from OEM post installation of the Hardware. Highest Level of Proactive and Reactive support covering Half yearly Firmware analysis, and Proactive Health analysis. All the disk/SSD/NVME components (Data Drives) including faulty disk components will be property of the bank and will not be returned to OEM/SI. | Herewith requesting Bank to amend as below : 5 Years 24/7 Warranty with 30 minutes Response Time and 6 hours Call to Resolution including part replacement, access to OEM support portal, OEM technical support on 24X7X365 basis. Successful Bidder must provide documentary proof from OEM post installation of the Hardware. All the disk/SSD/NVME components (Data Drives) including faulty disk components will be property of the bank and will not be returned to OEM/SI. | Please refer to the amendments. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 88 | 142 | 16.10. | General Requirements, Corrigendum | **RFP Clause:** All the devices/products/solutions proposed for this RFP should not be announced End of Life, End of Service Life for seven years from the date of submission of this RFP. **Corrigendum Clause:** "All the devices/products/solutions proposed for this RFP should not be announced End of Sale for two years from the date of the submission of the RFP and should be under OEM Support for 7 years from the date of the submission of the RFP" | OEM's practice of releasing updated models annually, it is not feasible to commit that the proposed products will not be declared End of Life (EOL) over a seven-year period. However, the OEM does guarantee End of Service Life support for five years from the End of Sale date, which includes continued technical support and critical updates. The products proposed are currently part of the active portfolio with no EOL/EOSL announcements.hence we request to reconsider this RPF clause. | Please adhere to the terms and conditions of RFP. |
| 89 | 165 | 7 | Annexure-X - Damages | The provisions of this Contract are necessary for the protection of the business goodwill of the parties and are considered by the parties to be reasonable for such purposes. Both the parties agree that any breach of this Contract will cause substantial and irreparable damages to the other party and, therefore, in the event of such breach, in addition to other remedies, which may be available, the party violating the terms of Contract shall be liable for the entire loss and damages on account of such disclosure. Each party agrees to indemnify the other against loss suffered due to breach of contract / RFP / SLA and undertakes to make good the financial loss, Litigation charges, Arbitration Charges, other charges etc caused directly or indirectly by claims brought about by its customers or by third parties. | | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 90 | 169 | 13 | Annexure-XIII | S.No Item Make/ Model/ Part Number<br>(To be specified by<br>the bidder) Multiplic- ation Factor (if any) HA<br>(within site) RAM Storage (Size in GB)<br>Operating System Database Additional Parts/<br>Modules along with Remark, if any<br>vCPU Clock Speed (GHz) Memory size in GB<br>1 NTP solution 2<br>(DC-1 & DR-1) NA<br>2 Asset Management solution 2<br>(DC-1 & DR-1) NA<br>3 Patch Management solution 2<br>(DC-1 & DR-1) NA<br>4 VAS 2<br>(DC-1 & DR-1) NA<br>5 Firewall management solution 2<br>(DC-1 & DR-1) NA<br>6 AV & EDR 2<br>(DC-1 & DR-1) NA<br>7 Web proxy 4<br>(DC-2 & DR-2) Required<br>8 NAC 4<br>(DC-2 & DR-2) Required<br>9 HIPS 2<br>(DC-1 & DR-1) NA<br>10 Data classification tool 2<br>(DC-1 & DR-1) NA<br>11 SIEM 4<br>(DC-2 & DR-2) Required<br>12 DAM 2<br>(DC-1 & DR-1) NA<br>13 Data Leakage prevention solution for end<br>points 2<br>(DC-1 & DR-1) NA | In the Annexure-XIII, WAF, Internal Firewalls & External Firewalls are missing. But, Firewall management has been asked, please clarify. | It is clarified that the annexure XIII is to mention the hardware requirements for running software components of CSOC solutions. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 91 | 16,21,26, 36,37 | Section D Page 16, Section E Page 21, Section D Page 26, Section 3 Page 26, Section D Page 36, Section 2.A Page 37 | | Things to be done at no additional cost to the bank: replace the solution (section d page 16), team to be deployed at any location (section e page 21), patches etc (section d page 26), upgrades (section 3 page 26, section d page 36), FM services is the bank/ bidder changes the solution (section 2.a page 37), etc | Bidder's scope shall be limited to the items expressly set out in the proposal. Any changes to the scope shall be subject to a mutually agreed Project Change Request in writing setting out the changes in the scope and related changes in timelines, commercials, and other implications | Please adhere to the terms and conditions of RFP. |
| 92 | 38,39,40 | Section K Page 38, Section L Page 39, Section H Page 40, Etc | INDIVIDUAL ROLE & RESPONSIBILITIES OF ONSITE, OFFSITE AND ONCALL TECHNICAL SUPPORT RESOURCES | Compliance with regulatory requirements | We request the following be clarified:<br><br>Client will comply with all laws and regulations applicable to it, and its own policies, from time to time ("Client Compliances"). If Client requires any change to the expressly stated scope items to comply with Client Compliances, Client will identify the changes required ("Client Compliance Directive") and will guide IBM on how to comply with the Client Compliance Directive. In case of any such change, IBM will propose modifications to the project to comply with the Client Compliance Directive, and such modifications shall be addressed via a mutually agreed change request setting out the changes to the scope, pricing, timelines and other related matters. Client retains authority and responsibility for determining that the project complies with the Client Compliances. | Please adhere to the terms and conditions of RFP. |
| 93 | 8, 14, 147 | Section 3 Page 8, Section "Technical Bid" Page 14, Annexure I Page 147 | Deviations not allowed | Deviations not allowed | We understand that the clarifications contained in the bidder's proposal will form part of the contract, such that in case of a conflict between the RFP and the bidder's proposal, the bidder's proposal will prevail | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 94 | | Corrigendum - Addendum | Annexure XVI | Annexure XVI | Annexure XVI only has 12 solutions mentioned, whereas the RFP ask if for 16 solutions. | It is clarified that this is pertaining to solutions only. Please adhere to the terms and conditions of RFP. |
| 95 | New | Additional query | | Additional Query | Requesting Bank to **Include Endpoint Sandboxing Solution which can be leveraged by EDR and Server Security solution.**<br><br>**Justification:** The EDR solution will work at its best when EPP, EDR and Sandboxing deployed together, it is industry best practice and bank will see the Maximum effectiveness of the EDR solution. The analysis process is divided into two ways to identify the anomalies - Static and Dynamic analysis.<br><br>For Static Analysis, the signature-based analysis is done by EPP first followed by the Behaviour based detection by EDR. If the malware is still unidentified (which is Zero-day vulnerability), then the Dynamic analysis will take place which will be performed by Sandboxing solution.<br><br>All these activities must happen one after another, hence it is very important to have all the solutions integrated tightly with each other and from the same OEM from day one and AV and EDR must be a single agent and single management console. **Indian bank is already using AV , EDR and Sandbox from same Vendor.** | Please adhere to the terms and conditions of RFP and Amendment. |
| 96 | New | Additional query | | Additional Query - PRE-QUALIFICATION CRITERIA OF THE OEM | OEM should have provided On-prem AV and EDR solution with minimum 10,000 endpoints in five Government Organizations/ BFSI / PSU in India, during last 5 years as on date of submission of Bids. Provide copies of completion certificate/ reference letter | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. | |
| 97 | New | Additional query | | Additional Query - PRE-QUALIFICATION CRITERIA OF THE OEM | OEM should have provided On-prem AV and EDR solution with minimum 10,000 endpoints in five Government Organizations/ BFSI / PSU in India, during last 5 years as on date of submission of Bids. Provide copies of completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. | Please adhere to the terms and conditions of RFP. |
| 98 | New | Additional query | | Additional Query - PRE-QUALIFICATION CRITERIA OF THE OEM Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary | OEM should have provided On-prem AV and EDR solution with minimum 10,000 endpoints in five Government Organizations/ BFSI / PSU in India, during last 5 years as on date of submission of Bids. Provide copies of completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. | Please adhere to the terms and conditions of RFP. |
| 99 | New | Additional query | | Current Submission is 12th September. | Request you to give us the extension to submit the RFP for another 20 days from the date of corrigendum. As post corrigendum we need to take some interternal approval which will take some time and consolidating the reference as well. | Please refer to the amendments. |
| 100 | New | Additional query | | Submission Date -12.09.2025 | Request you to extend one more week. Submission date - 19.09.2025 | Accepted the extension of bid submission. Please refer to GEM portal for the updated date. |
| 101 | New | Additional query | | | If the bidder is required to provision OEM products and/or OEM support thereon (collectively “OEM Items”), those will be provided solely as per OEM terms. In case of any issues arising from OEM Items, bidder will coordinate with the relevant OEM or reseller to pass on | Please adhere to the terms and conditions of RFP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | any service level credit to XXXXX, but the bidder shall not be responsible for any representations, warranties or indemnities in respect of OEM Items. Notwithstanding anything contained in the RFP or the contract, under no circumstances shall bidder be liable for any damages arising out of use of OEM Items | |
| 102 | New | Additional query | | | Requesting Bank to **Include Endpoint Sandboxing Solution which can be leveraged by EDR and Server Security solution.**<br><br>**Justification:** The EDR solution will work at its best when EPP, EDR and Sandboxing deployed together, it is industry best practice and bank will see the Maximum effectiveness of the EDR solution. The analysis process is divided into two ways to identify the anomalies - Static and Dynamic analysis.<br><br>For Static Analysis, the signature-based analysis is done by EPP first followed by the Behaviour based detection by EDR. If the malware is still unidentified (which is Zero-day vulnerability), then the Dynamic analysis will take place which will be performed by Sandboxing solution.<br><br>All these activities must happen one after another, hence it is very important to have all the solutions integrated tightly with each other and from the same OEM from day one and AV and EDR must be a single agent and single management console. **Indian bank is already using AV , EDR and Sandbox from same Vendor.** | Please adhere to the terms and conditions of RFP and Amendment. |
| 103 | New | Additional query | | | kindly request an extension of two weeks to the current bid submission deadline | Please adhere to the terms and conditions of RFP and Amendment. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 104 | New | Additional query | | | Requesting Bank to **Include Endpoint Sandboxing Solution which can be leveraged by EDR and Server Security solution.**<br><br>**Justification:** The EDR solution will work at its best when EPP, EDR and Sandboxing deployed together, it is industry best practice and bank will see the Maximum effectiveness of the EDR solution. The analysis process is divided into two ways to identify the anomalies - Static and Dynamic analysis.<br><br>For Static Analysis, the signature-based analysis is done by EPP first followed by the Behaviour based detection by EDR. If the malware is still unidentified (which is Zero-day vulnerability), then the Dynamic analysis will take place which will be performed by Sandboxing solution.<br><br>All these activities must happen one after another, hence it is very important to have all the solutions integrated tightly with each other and from the same OEM from day one and AV and EDR must be a single agent and single management console. **Indian bank is already using AV , EDR and Sandbox from same Vendor.** | Please adhere to the terms and conditions of RFP and Amendment. |

# TAMIL NADU GRAMA BANK

**REF RFP No: TMD/3/2025-26 dated 28/07/2025**

## Amendments 2

| S. No. | Page No. | Clause No. | Type | Existing RFP clause | Amended RFP clause |
|---|---|---|---|---|---|
| 1 | 8 | 3.1 | PRE-QUALIFICATION CRITERIA OF THE BIDDER (Corrigendum - Amendments - Point 105) | Subsidiary companies may use financials of the parent company for demerging entities.<br>However, technical experience should be complied by the subsidiary company only i.e., bidding company only. | Subsidiary companies may use financials and technical experience of the parent company for demerging entities.<br>All the supporting documents/proof to be submitted and additionally Undertaking/Guarantee from parent company clearly stating technical experience of the persons deploying the project to be disclosed.<br>(Please refer addendum. Annexure XVIII - To be submitted. ) |
| 2 | 10 | 5.m | OTHER CONDITIONS | The successful bidder should provide SBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of contract. Solution should be comprehensive in nature. | The successful bidder / OEM of the proposed solution should provide SBOM & CBOM for all the products quoted. Bidder should ensure that all the components of SBOM are appropriately licensed and supported by corresponding OEM. Intellectual property rights to be properly checked by the bidder and bidder holds responsibility for the IPR of solutions deployed. Also, should ensure that the SBOM is free of vulnerabilities during the period of contract. Solution should be comprehensive in nature. |
| 3 | 16 | 14 | EVALUATION AND AWARD CRITERIA | Additional Clause | Evaluation of Bids:<br>Even if the POC is qualified and during implementation if the RFP specifications are not met, then the OEM/bidder will be required to replace the subjected solution/product with a better proven solution/product at no additional cost to the Bank, within the stipulated timelines. The OEM name of the alternate solution should be mentioned in Annexure-XVII. However, MAF and customer references for the alternate solution may be provided before its implementation. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 23 | I | Hardware/Solution Uptime | Group-II Response time:<br>If number of end points reporting goes below 95%, it must be made to report to Central site within 8 hours. Penalty will be levied based on the number of end points not reporting for more than 8 hours. Penalty will be applicable for<br>number of endpoints not reporting beyond 8 hours and it will be calculated on monthly average.<br>At least 95% of endpoints should be communicating to central solution console for a particular day. Out of these reporting 95% Endpoints, 95% endpoints should be updated with latest versions as applicable.<br>100% of endpoints should report during each month to central site solution.Uptime will be calculated on monthly basis.Penalty amount in % will be calculated on Cost of respective solution including AMC/ATS (except<br>Facility Management and Implementation Charges) for 5years. | Group-II Response time:<br>If number of end points reporting goes below 98%, it must be made to report to Central site<br>within 8 hours. Penalty will be levied based on the number of end points not reporting for more than 8 hours. Penalty will be applicable for number of endpoints not reporting beyond 8 hours and it will be calculated on monthly average. At least 98% of endpoints should be communicating to central solution console for a particular day. Out of these reporting 98% Endpoints, 95% endpoints should be updated with latest versions as applicable. 100% of endpoints should report during each month to central site solution.<br>Uptime will be calculated on monthly basis. Penalty amount in % will be calculated on Cost<br>of respective solution including AMC/ATS (except Facility Management and Implementation Charges) for 5 years |
| 5 | 25 | VI.a | Penalties related to Facility Management/ Onsite Technical Support | The onsite engineer should be available at DC/DR/Any other location as per the shift schedule, irrespective of Holiday of the Bidder company. The engineers should be punctual and sign on the register provided at the office. In the case of unauthorized absence, and if suitable resource with similar skillset is not deployed on<br>the day of absence, FM payment for the period of absence will not be paid and in addition to that, a penalty of amount equivalent to the cost of the resource per day of absence will be levied for the absent period. Holidays/off days, if any, clubbed in between the period of absence and holidays/off-days preceding or succeeding the<br>absence period will also be counted in the period of absence while calculating penalty. | The onsite engineer should be available at DC/DR/Any other location as per the shift schedule, irrespective of Holiday of the Bidder company. The engineers should be punctual and sign on the register provided at the office.<br><br>In case engineer is on leave/absent, alternate engineer should be available in a similar skillset/same capacity for the shift to run the routine operations and smooth functioning of CSOC. If suitable resource is not deployed on the day of leave/absent, it will attract penality of Rs.10,000/- per day per person. No shift should remain unmanned.<br><br>Holidays/off days, if any, clubbed in between the period of leave/ absence and holidays/ off-days preceeding or |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | succeeding the absence period will also be counted in the period of absence while calculating penality. |
| 6 | 45 | 1.13 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should support Role-based administrative access and also MFA for the same | The Firewall solution should support Role-based administrative access and also integrate with any MFA solutions |
| 7 | 46 | 1.15 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS -INTERNAL FIREWALL | The Firewall solution should support import and export of security policies (in .csv and .xls files) \configurations without any downtime | The Firewall solution should support import of security policies\configurations through API and export of security policies in different file formats like.csv, .pdf without any downtime |
| 8 | 59 | 3.56 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM | The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier. | Clause removed |

| | | | | | |
|---|---|---|---|---|---|
| 9 | 78 | 6.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - CLMS, Corrigendum | **RFP Clause:** The retention duration should be flexible ( current requirement is 5 years for VPN logs and 1 year for other logs).<br>**Corrigendum Clause:** (469) Please adhere to the terms and conditions of RFP.<br>**RFP Clause :**<br>• Bidder to provide 200 licenses for log management solution.<br>• DC and DR setup for the solution to be implemented without HA.<br>• However the log sources may be at various locations as required by bank<br><br>**Corrigendum Clause:** It is a Greenfield Implementation and device details will be shared with successful bidder. The rolling log retention period for CLMS is as follows<br>online: 270 days<br>offline: Bank will provide tape back up infrastructure. | The retention duration should be flexible. The current rolling log retention period for CLMS is as follows online: 270 days, offline: Bank will provide tape back up infrastructure.<br>Any hardware/software required may be sized accordingly. |
| 10 | 82 | 7.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux .<br><br>**Amended Clause**: "The proposed solution must support OS versions<br>like Windows, Linux Versions like RHEL and<br>Oracle Linux ." | The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux.<br><br>In case the AV & EDR supports only Windows Operating System, a separate application may be quoted for the specification to operate on Linux endpoints. Ratio of Windows: Linux may be treated as 29:1 |
| 11 | 85 | 7.2.19 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | Proposed solution agent upgrade process must be completely invisible to end-users. The process must not require restarting servers, hosts, endpoints and should not prompt end users for any actions. | The proposed solution agent upgrade process must be completely invisible to end-users. The process may require restart of servers, hosts, endpoints only in exceptional cases. |

| | | | | | |
|---|---|---|---|---|---|
| 12 | 85 | 1.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | The proposed solution should be able to support Windows, MAC, Ubuntu and Linux (all flavours like Oracle, RHEL etc) operating systems.<br><br>**Amended Clause:** "The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux ." | The proposed solution must support OS versions like Windows, Linux Versions like RHEL and Oracle Linux.<br><br>In case the AV & EDR supports only Windows Operating System, a separate application may be quoted for the specification to operate on Linux endpoints. Ratio of Windows: Linux may be treated as 29:1 |
| 13 | 88 | 7.2.45 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - EDR with AV, ENDPOINT DETECTION & RESPONSE (EDR) | 2.45 The proposed solution should have the option to block the intruder hosts for a specific number of seconds.<br><br>**Amended Clause:** "The proposed solution should have the option to block/isolate/quarantine the intruder hosts for a specific number of seconds." | The proposed solution should have the option to block/isolate/quarantine the intruder hosts. |
| 14 | 89 | 4.8 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - ENDPOINT PROTECTION PLATFORM (EPP)/ANTI VIRUS FOR ENDPOINTS(AV) | Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | Solution should prevent execution of tampered applications. |
| 15 | 104 | 11.1.1 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Bidder is responsible for providing necessary software licenses in HA mode in both DC and DR locations. Capability to failover shall be made available at both locations. Bank will Provide Necessary VM resources to deploy and run the solutions. | Bidder is responsible for providing necessary software licenses in HA mode in both DC and DR locations. Capability to failover shall be made available at both locations. |
| 16 | 105 | 11.2.12 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, all service running, all process running, all application version, all application installed etc. to achieve 100% device visibility with NAC. | Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, all application version, all application installed etc. to achieve 100% device visibility with NAC. |

| | | | | | |
|---|---|---|---|---|---|
| 17 | 105 | 11.2.6 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Works via agent-less, persistent client-based agent and a dissolvable/temporary agent to validate that an endpoint is conforming to a company's posture policies which includes but not limited to checks for the latest OS patches, antivirus/EDR and antispyware software packages with current definition version, Windows registries key, Windows registry value, Linux process etc., and applications, local firewalls, P2P applications, Disk Encryptions, USB Check, etc. | Works via agent-less, persistent client-based agent and a dissolvable/temporary agent to validate that an endpoint is conforming to a company's posture policies which includes but not limited to checks for the latest OS patches, antivirus/EDR and antispyware software packages with current definition version, Windows registry key or Windows registry value, Linux process etc., and applications, local firewalls, P2P applications, Disk Encryptions, USB Check, etc. |
| 18 | 105 | 11.2.11 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The NAC solution must bi-directionally integrate with SCCM. Perform posture assessment based on various properties like Advertisement List, Collection List, Last Hardware Inventory List, SCCM Client Software GUID, Software Updates List etc. and help auto remediation SCCM client with new advertisements and then update the SCCM server with the new status. | The NAC solution must integrate with SCCM to support posture assessment based on SCCM client status. The solution should be able to trigger SCCM evaluation on endpoints and assess compliance based on SCCM-reported software update status and other posture-related criteria. |
| 19 | 105 | 11.2.15 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The solution should provide out of the box visibility to Virtual machine properties such as Boot Time, Virtual Machine Hardware, is Virtual Machine orphan, Virtual Machine Peripheral Devices info, Virtual Machine port group, Virtual Machine power state, Virtual Machine CPU usage, Virtual Machine usage network I/O (KBPS) etc | Clause removed |
| 20 | 106 | 11.2.16 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must support controlling capabilities of USB devices (with Class level detectionof Peripheral Devices like printer, imaging devices, WPD, Bluetooth, etc.) with and without endpoint agents. | Solution must support controlling capabilities of USB devices (with Class level detectionof Peripheral Devices like printer, imaging devices, WPD, Bluetooth, etc.) with or without endpoint agents. |
| 21 | 106 | 11.2.17 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Provides the ability to create powerful posture assessments policies by checking availability of latest OS patches, antivirus, EDR and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications. | Provides the ability to create powerful posture assessments policies by checking availability of latest OS patches, antivirus, EDR and antispyware software packages with current definition file variables (version, date, etc.), registries key/value etc, and applications. |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 106 | 11.2.24 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Proposed solution should verify access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers, TACACS+ etc. It shall allow enforcement of identity- based policies after an element is allowed in the network. | Proposed solution should verify access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers or TACACS+ etc. It shall allow enforcement of identity-based policies after an element is allowed in the network. |
| 23 | 106 | 11.2.25 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The Solution should provide a highly powerful and flexible attribute-based accesscontrol solution that combines authentication, authorization, posture, profiling, and guest management services on a single platform. | The Solution should provide a highly powerful and flexible attribute-based accesscontrol solution that combines authentication, authorization, posture, profiling, and guest management services on a single OEM platform. |
| 24 | 107 | 11.5.4 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must automate the inventorying of IP-connected assets across extended enterprise networks along with detailed information of hardware viz. Disks, Display Units, Motherboard, Network Adapter, Physical Memory, Plug and Play Device, Processor, etc continuously and accurately for all connected devices. | Solution must automate the inventorying of IP-connected assets across extended enterprise networks for all connected devices. |
| 25 | 107 | 11.5.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must be able to provide compliance for Hardware properties on windows like<br>Hardware Computer, Disks, Display Unit, Motherboard, Network Adapter, Physical Memory, Plug and Play Device, Processor, etc. | Solution must be able to verify compliance for Hardware properties on windows like<br>Hardware Computer, Disks, Display Unit, Motherboard, Network Adapter, Physical Memory, Plug and Play Device, Processor, etc. either natively or through integration. |
| 26 | 107 | 11.3.6 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The proposed NAC solution should detect devices with missing or broken SCCM agents before allowing network access. It should be able to automatically enroll devices with missing agents at the connection time and leverage SCCM for automated agent deployment. It must be able to leverage SCCM host properties within the NAC policies. Further, it must be able retrieve advertisements (Patch and Software update) related to SCCM hosts, update SCCM clients with new advertisements (Patch and Software | The NAC solution must integrate with SCCM should detect devices with missing or broken SCCM agents before allowing network access. It should be able to automatically enroll devices with missing agents at the connection time and leverage SCCM for automated agent deployment. It must be able to leverage SCCM host properties within the NAC policies. Further, it must be able retrieve advertisements (Patch and Software update) related to SCCM hosts, update SCCM clients with new advertisements (Patch and Software update), and update the SCCM server with new host information. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | update), and update the SCCM server with new host information. | |
| 27 | 107 | 11.3.7 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | The proposed NAC solution should be able to provide capability to run custom scripts on Windows endpoints to meet endpoint compliance. (For Example, but not limited to endpoints chassis type, Free Space in C drive or Windows Activation status details etc.) or for auto- remediation (For Example Uninstalling Blacklisted application, Kill Blacklisted process, installing security host-based agent etc.) | The proposed NAC solution should integrate with endpoint management or security platform to meet endpoint compliance. |
| 28 | 108 | 11.6.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Solution must support capability to generate report for hardware (Memory, RAM, HDD, Peripheral devices, etc.), all installed software with version, Open ports (TCP/UDP), Service Running, Process Running and application inventory across managed extended enterprise. | Solution must support capability to generate reports for device inventory, installed applications with version and device classification (OS, MAC, IP, vendor, type). Customizable reporting and alerting through built-in tools and/or integration. |
| 29 | 108 | 11.6.5 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network. | Includes a web console from the same OEM for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network. |
| 30 | | | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - NETWORK ACCESS CONTROL (NAC) | Additional Clause | The solution should be vendor agnostic and should not only rely upon 802.1x integration. |
| 31 | 112 | 13.20. | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should display icons over files that have been classified using the solution. | The solution should have a feature to identify both classified and unclassified files. |

| | | | | | |
|---|---|---|---|---|---|
| 32 | 113 | 13.27 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Data Classification | The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy. | The solution should provide suggestions based on the content for doing manual classification of data. |
| 33 | 141 | 16.2.3 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS - Hosting Infrastructure - Server - Warranty | 5 Years 24/7 Warranty with 30 minutes Response Time and 4 hours Call to Resolution including part replacement, access to OEM support portal, OEM technical support on 24X7X365 basis. Successful Bidder must provide documentary proof from OEM post installation of the Hardware. Highest Level of Proactive and Reactive support covering Half yearly Firmware analysis, and Proactive Health analysis. All the disk/SSD/NVME components (Data Drives) including faulty disk components will be property of the bank and will not be returned to OEM/SI. | 5 Years 24/7 Warranty with 30 minutes Response Time and 6 hours Call to Resolution including part replacement, access to OEM support portal, OEM technical support on 24X7X365 basis. Successful Bidder must provide documentary proof from OEM post installation of the Hardware. All the disk/SSD/NVME components (Data Drives) including faulty disk components will be property of the bank and will not be returned to OEM/SI. |
| 34 | 141 | 10 | General Requirements | **Amended Clause:** All the devices/products/solutions proposed for this RFP should not be announced End of Life, End of Service Life for seven years from the date of submission of this RFP. | Bank requires minimum 7 years support period from date of submission of this RFP.<br>Declaration from O.E.M to be submitted separately for all devices/products/solutions. |
| 35 | New | Additional query | GENERAL TENDER DETAILS | Current Submission is 12th September. | Last date and time for Online bid submission (both Technical & Commercial): 24-09-2025 |

# TAMIL NADU GRAMA BANK

**REF RFP No: TMD/3/2025-26 dated 28/07/2025**

**ANNEXURES (REVISED)**

## Annexure-XVI

## 16.REVISED CHECKLIST FOR DOCUMENTS TO BE SUBMITTED WITH TECHNICAL BID

**[SETTING UP OF CYBER SECURITY OPERATION CENTER (CSOC) IN TNGB AND PBGB]**

**REF: TMD/3/2025-26 dated 28/07/2025**

The technical bid document should mandatorily comprise of the following:

| S.No. | Description of Documents required | Remarks |
|---|---|---|
| 1 | EARNEST MONEY DEPOSIT (EMD) | TO BE SUBMITTED IN ORIGINAL |
| 2 | COPY OF CERTIFICATE OF INCORPORATION OR ANY OTHER CERTIFICATE OF REGISTRATION ISSUED BY COMPETENT AUTHORITY FROM GOVERNMENT OF INDIA. | DOCUMENTS TO BE SUBMITTED |
| 3 | CERTIFIED COPY OF ISO 27001:2013 (OR LATER) CERTIFICATES | DOCUMENTS TO BE SUBMITTED |
| 4 | PERFORMANCE CERTIFICATE & PO SUPPORTING THE CLAIM FROM THE RESPECTIVE ORGANIZATION SHOULD BE SUBMITTED ALONG WITH CONTACT DETAILS OF THE COMPANY. | DOCUMENTS TO BE SUBMITTED |
| 5 | AUDITED FINANCIAL STATEMENTS FOR THE LAST THREE (3) FINANCIAL YEARS I.E., FY2022-23, FY2023-24 and FY 2024-25. | DOCUMENTS TO BE SUBMITTED |
| 6 | BOARD RESOLUTION IN FAVOUR OF AUTHORIZED PERSON AND POWER OF ATTORNEY/ AUTHORIZATION LETTER (FROM AUTHORIZED PERSON EXECUTED ON STAMP PAPER OF APPROPRIATE VALUE) | DOCUMENTS TO BE SUBMITTED |
| 7 | THE BIDDER MUST HAVE THEIR SOC IN INDIA PROVIDING SECURITY SERVICES TO VARIOUS PUBLIC/PRIVATE COMPANIES/ORGANISATIONS | DOCUMENTS TO BE SUBMITTED |
| 8 | OTHER PRE QUALIFICATION CRITERIA – ELIGIBILITY PROOF and COMPLIANCE DECLARATION | DOCUMENTS TO BE SUBMITTED |
| 9 | TECHNICAL AND FUNCTIONAL SPECIFICATIONS | As per Specifications and allied technical details section |
| 10 | BID FORM | Annexure I of RFP |
| 11 | INTEGRITY PACT | Annexure II of RFP |
| 12 | BIDDER'S INFORMATION | Annexure III of RFP |
| 13 | PERFORMANCE CERTIFICATE | Annexure IV of RFP |
| 14 | UNDERTAKING FOR NON- BLACKLISTED | Annexure V of RFP |
| 15 | TURNOVER CERTIFICATE NETWORTH CERTIFICATE | Annexure VI of RFP |
| 16 | MANUFACTURER'S (OEM) AUTHORISATION FORM | Annexure VII of RFP |
| 17 | FORMAT FOR BID SECURITY BANK GUARANTEE | Annexure VIII of RFP |
| 18 | FORMAT FOR PERFORMANCE BANK GUARANTEE | Annexure IX of RFP |
| 19 | NON-DISCLOSURE AGREEMENT | Annexure X of RFP |
| 20 | UNDERTAKING OF INFORMATION SECURITY FROM THE BIDDER | Annexure XI of RFP |
| 21 | ESCALATION MATRIX | Annexure XII of RFP |

| | | |
|---|---|---|
| 22 | HARDWARE REQUIREMENTS FOR THE OFFERED SOLUTIONS | Annexure XIII of RFP |
| 23 | CONTRACT FORM | Annexure XIV of RFP |
| 24 | Training Details | Annexure XV of RFP |
| 25 | REVISED CHECKLIST FOR DOCUMENTS TO BE SUBMITTED WITH TECHNICAL BID | Annexure XVI of RFP |
| 26 | FORMAT FOR CONFIRMING THE SOLUTION TO THE BID | Annexure XVII of RFP |
| 27 | UNDERTAKING FROM PARENT COMPANY - Applicable only to participation of demerged entities (by virtue of a corporate demerging etc.) | Annexure XVIII of RFP |
| 28 | BIDDER - Office Details with Address and Contact for Technical Support in Chennai | PROOF/DOCUMENTS TO BE SUBMITTED |
| 29 | OEM - Proof for having Technical support center in India | PROOF/DOCUMENTS TO BE SUBMITTED |
| 30 | SIEM – Installation Proof | PROOF/DOCUMENTS TO BE SUBMITTED |
| 31 | Declaration for minimum 7 years support from O.E.M for all devices/products/solutions | DOCUMENTS TO BE SUBMITTED from O.E.M in addition to MAF |

**Annexure XVII**

**17. FORMAT FOR CONFIRMING THE SOLUTION TO THE BID**

| S.No | Item Description | Primary Solution | | | | Secondary Solution*** in case of primary solution is not working within the first year of post implementation of the software | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Name of Software | O.E.M | Subscription/ Perpetual | License Qty | Name of Software | O.E.M | Subscription/ Perpetual | License Qty |
| 1 | Database Activity Monitoring (DAM) Solution | | | | | | | | |
| 2 | Asset Management | | | | | | | | |
| 3 | Patch Management | | | | | | | | |
| 4 | Centralized Log Management Solution (CLMS) | | | | | | | | |
| 5 | Web Proxy Solution | | | | | | | | |
| 6 | Security Incident and Event Management (SIEM) | | | | | | | | |
| 7 | AV and Endpoint Detection Response | | | | | | | | |
| 8 | Network Access Control (NAC) | | | | | | | | |
| 9 | VAS | | | | | | | | |
| 10 | HIPS | | | | | | | | |
| 11 | Data classification | | | | | | | | |
| 12 | Data Leakage prevention solution for end points | | | | | | | | |

***Secondary solution should be provided by the O.E.M of primary solution and the bidder without any additional cost to the Bank.

Compatibility with hardware provided in this RFP has been maintained.

All licenses at DC/DR with high availability have been factored.

All other RFP delivery & implementation conditions have been adhered.

Yours faithfully,

**Signature of Authorized Signatory (of Bidder)**

Name of Signatory:
Designation:
Date:
Place:
Email ID:
Mobile Number:
Telephone No.:
Seal of the Company:

**Annexure XVIII**

**18. UNDERTAKING FROM PARENT COMPANY**

**[SETTING UP OF CYBER SECURITY OPERATION CENTER (CSOC) IN TNGB AND PBGB]**

**REF: TMD/3/2025-26 dated 28/07/2025**

We _____as a parent company (referred as "company 1") of _____ (subsidiary company/demerged entity) (referred as "company 2") provide our confirmation to use the experience of both financials and technical of company 1 by company 2 for this tender.

Upon "Company 2" being declared successful in the tender evaluation process, the "Company 1" shall execute a tripartite agreement of guarantee in favour of the Bank, undertaking to be liable for any loss, damage, or expense that may be caused to Banks (TNGB & PBGB) as a result of Company 2's failure to duly perform or provide the services under the tender/contract.

Date:

Place:

**[Signature of Authorized Signatory of Parent Company]**

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

*Proof of Authorised signatory to be submitted.