

**NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT  
MUMBAI**

**Request for Proposal  
For  
Supply, Installation, Configuration, Testing, Commissioning and  
Maintenance of  
“Next Generation Firewall Appliances”**

This Document, containing 110 pages, is the property of National Bank for Agriculture and Rural Development (NABARD). The use of the contents of this document, even by the Authorized personnel or agencies for any purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian Law.



## General Information

1. The RFP is posted on NABARD's website [www.nabard.org](http://www.nabard.org). NABARD reserves the right to change the requirements. Any changes made subsequently will be posted only on the web site. Hence before submitting bids, bidder must ensure that such clarifications/changes have been considered by them. NABARD will not have any responsibility in case some omission is done by any bidder.
2. Bidders are advised to study the bid document carefully and submit the bids. The submission shall be deemed to have been done after careful study and examination of the bid document with full understanding of its implications.
3. A bidder cannot bid for more than one product of Next Generation Firewall. If violated, all the bids submitted by the bidder will be rejected.
4. Either the bidder on behalf of the OEM or OEM itself can bid but both cannot bid simultaneously for the solution.
5. NABARD has both Checkpoint & SonicWALL firewall in the core, hence for perimeter firewall Banks intends to have different make firewall i.e. Checkpoint & SonicWALL firewall should not be quoted.
6. In case OEM is a bidder, an undertaking that the OEM shall provide Direct Premium support directly for the supplied hardware and software. The same need to be provided as undertaking.
7. In case SI is a bidder, an undertaking from OEM needs to be provided by SI that the concerned OEM shall provide Direct Premium support for the supplied hardware and software.
8. Only the latest but stable version/model of Hardware, Software, firmware etc. should be proposed indicating the version/model number and other relevant details clearly.
9. Bidder must ensure that the end of life of the product should be at least three years and end of support at least six years from the last date or extended last date of submission of the RFP.
10. Each page of the technical as well as commercial bid and any supplementary document attached, if any, should have the signature and the seal of an authorized person.
11. The participating bidders are required to submit documentary evidence in support of all the eligibility criteria.
12. All the information/documents sought through the RFP should be provided. Incomplete information/documents may lead to rejection.
13. In case of any clarification required by NABARD to assist in the examination, evaluation and comparison of bids, NABARD may, at its discretion, ask the bidder for clarification. The response / clarification shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.
14. Any clarifications sought by the NABARD or the bidders will be published on website or shared by email, if NABARD thinks it fit to do so.
15. Bids once submitted will be treated as final unless clarifications are sought by NABARD.
16. NABARD reserves the right to impose a penalty, if the successful bidder chooses to withdraw the bid.
17. NABARD shall not be responsible for non-receipt/non-delivery of bid documents due to any reason.
18. The Last date of Submission of bid is **06 December 2017 at 1400 Hrs.**
19. The response to the RFP should be in English only.
20. All prices should be quoted in Indian Rupees only.

21. Notwithstanding anything contained herein above, in case of any dispute, claim and legal action arising out of this RFP, the parties shall be subject to the jurisdiction of courts at Mumbai, Maharashtra, India only.
22. Bidder is required to sign the Integrity Pact during the bidding process as per the Format attached.
23. Any publicity by the Service Provider in which the name of the Bank is to be used, will be done only with the explicit written permission of the Bank.
24. The Bank shall be under no obligation to accept the lowest or any other offer received in response to this tender notice and shall be entitled to reject any or all tenders without assigning any reason whatsoever.
25. After the selection process, the successful bidder should be prepared to revise the proposal, if need be, to fit the stated objectives of NABARD. At the end of these discussions, NABARD will notify the award of contract and forward format of Service Level Agreement (SLA) to the selected bidder.
26. The successful Bidder should submit the SLA on the stamp paper of requisite value and return it to NABARD within 14 days of receipt of notification.
27. Selected vendor should not enter into any sub -contract for entrusting a part or entire scope of work to any other vendor or party.
28. The SLA shall be written in English. All correspondence and other documents pertaining to the SLA, which will be exchanged by the parties, shall also be written in English.
29. NABARD has the right to reject any or all bids received without assigning any reason whatsoever.

## Schedule of events :

|    |   |   |
|----|---|---|
| 1  | Purpose   | The purpose of this RFP is to invite techno-commercial bids from Private/Public Ltd Companies/Public undertaking/partnership Vendors, for the Product fulfilling the functionalities as outlined in the Scope of Work & Annexure VII of this document.  |
| 2  | Cost of Bid   | ₹10,000/- (Rupees Ten Thousand Only) in the form of Demand Draft.   |
| 3  | EMD   | ₹1,00,000/- (Rupees One Lakh Only) to be submitted as Bank Guarantee/Pay Order/ Demand Draft drawn on Commercial bank in favour of NABARD   |
| 4  | No. of Envelopes (Non window & sealed) to be submitted            | Two (2) Envelopes<br><b>Envelope 1 containing:</b><br>1. Technical Bids containing technical response & all Annexures except Annexure IX & XVII.<br>(Submmit 1 hard copy and 1 soft copy in CD)<br>2. DD towards cost of RFP & DD/BG/Pay Order for EMD.<br><b>Envelope 2 containing:</b><br>Commercial Bid as per Annexure IX & X (Only one bid to be kept).<br>(Submmit 1 hard copy and 1 soft copy in CD) |
| 5  | Last Date of Submission of Bids                                   | <b>06 December 2017, 14:00 hrs</b>  |
| 6  | Date, Time and Venue of opening of Bids, except Commercial Bids.  | 06 December 2017, 14:30 hrs<br>Department of Information Technology, Fifth Floor, C Wing, NABARD, Head Office, C-24, G-block, Bandra- Kurla Complex, Bandra – (East), Mumbai 400051   |
| 7  | Last Date of query Submission                                     | <b>22 November 2017, 11:00 hrs</b>  |
| 8  | Pre-bid meeting   | <b>24 November 2017, 14:00 hrs</b>  |
| 9  | Response to clarification / pre bid meeting to be put on web site | <b>27 November 2017, 15:00 hrs</b>  |
| 9  | Bid Validity  | 180 days from the last date of submission.  |
| 10 | Address for submission of Bids                                    | Chief General Manager,<br>Department of Information Technology,<br>Fifth Floor, C Wing, NABARD, Head Office,<br>C-24, G-block, Bandra - Kurla Complex<br>Bandra (East), Mumbai 400051   |
| 11 | Contact Persons :   | Ms. Sujatha Sudhindran, DGM, DIT, NABARD<br>Shri Satish Kumar Singh, Mgr, DIT, NABARD   |



## Contents

|  |    |
|--|----|
| Schedule of events : .....                           | 4  |
| Contents .....                                       | 5  |
| <b>1 Introduction</b> .....                          | 9  |
| <b>2 Purpose of RfP</b> .....                        | 9  |
| 2.1 Information Provided.....                        | 9  |
| 2.2 Disclaimer .....                                 | 9  |
| 2.3 Costs to be borne by bidder .....                | 9  |
| 2.4 No Legal Relationship .....                      | 10 |
| 2.5 Bidder’s Obligation to Inform Itself .....       | 10 |
| 2.6 Evaluation of Offers .....                       | 10 |
| 2.7 Errors and omissions .....                       | 10 |
| 2.8 Acceptance of Terms & Conditions.....            | 10 |
| 2.9 Lodgment of RFP .....                            | 10 |
| 2.9.1 RFP submission:.....                           | 10 |
| 2.9.2 RFP Validity Period.....                       | 12 |
| 2.9.3 Queries regarding “Request for Proposal” ..... | 12 |
| 2.10 Notification .....                              | 12 |
| 2.11 Disqualification.....                           | 12 |
| 2.12 Definition .....                                | 12 |
| 2.13 Bid Currency.....                               | 14 |
| <b>3 Background</b> .....                            | 14 |
| 3.1 About NABARD .....                               | 14 |
| 3.2 Present IT set up.....                           | 15 |
| <b>4 Scope of Work</b> .....                         | 15 |
| 4.1 Project Objective.....                           | 15 |
| 4.2 Project Plan.....                                | 18 |
| 4.2.1 SRS & Gap Analysis.....                        | 19 |
| 4.2.2 Kick –off.....                                 | 20 |
| 4.2.3 Deployment, Installation, Configuration .....  | 20 |
| 4.2.4 Testing.....                                   | 20 |



- 4.2.5 Go-live..... 20
- 4.2.6 Training ..... 20
- 4.2.7 AMC & Warranty ..... 20
- 4.3 Product Features ..... 21
- 4.4 Hardware..... 23
  - 4.4.1 Next Generation firewall:- ..... 23
  - 4.4.2 Management, Reporting & Logging H/w ..... 23
  - 4.4.3 Switches..... 23
  - 4.4.4 Miscellaneous ..... 24
- 4.5 Softwares ..... 24
  - 4.5.1 Licenses/subscription..... 24
  - 4.5.2 Operating System ..... 24
  - 4.5.3 Firmware ..... 24
  - 4.5.4 Database..... 24
  - 4.5.5 Miscellaneous ..... 24
- 4.6 Services ..... 25
  - 4.6.1 Implementation of Firewalls ..... 25
  - 4.6.2 Creation of DMZ in the existing network ..... 25
  - 4.6.3 Warranty, Extended Warranty, AMC & FMS..... 25
  - 4.6.4 On-Site Support ..... 27
  - 4.6.5 Preventive Maintenance..... 27
  - 4.6.6 End of Sale and End of Support ..... 28
  - 4.6.7 Training ..... 28
- 4.7 Requirement ..... 28
  - 4.7.1 Infrastructure ..... 28
  - 4.7.2 Software ..... 29
  - 4.7.3 Hardware..... 29
  - 4.7.4 Network requirements..... 29
  - 4.7.5 Management, Reporting & logging module..... 29
  - 4.7.6 Licensing..... 30
  - 4.7.7 System & Security Audit..... 30
  - 4.7.8 Testing ..... 30
  - 4.7.9 Installation Certificate..... 31
  - 4.7.10 Final Acceptance Certificate..... 31
  - 4.7.11 Go – live ..... 32



|        |  |    |
|--------|--|----|
| 4.7.12 | AMC, Warranty & Support .....                                      | 32 |
| 4.7.13 | Documentation and User Manual .....                                | 32 |
| 4.7.14 | Shifting of premise.....   | 33 |
| 4.7.15 | Others .....   | 33 |
| 4.7.16 | NABARD’s Responsibility.....                                       | 34 |
| 5      | <b>Pricing</b> .....   | 34 |
| 6      | <b>Payment</b> .....   | 34 |
| 7      | <b>Eligibility Criteria</b> .....                                  | 35 |
| 7.1    | Technical .....  | 35 |
| 7.2    | Financial : .....  | 36 |
| 8      | <b>Signatory</b> .....   | 37 |
| 9      | <b>Amendments of bidding documents</b> .....                       | 37 |
| 10     | <b>Pre-Bid Meeting</b> .....                                       | 37 |
| 11     | <b>Opening of Quotation</b> .....                                  | 37 |
| 12     | <b>Earnest Money Deposit (EMD)</b> .....                           | 38 |
| 12.1   | The EMD shall be forfeited if.....                                 | 38 |
| 13     | <b>Performance</b> .....   | 38 |
| 13.1   | Uptime Efficiency.....   | 39 |
| 13.2   | Response Time to errors .....                                      | 39 |
| 14     | <b>Spare parts</b> .....   | 40 |
| 15     | <b>Ethical Standard</b> .....                                      | 40 |
| 16     | <b>Information Security</b> .....                                  | 41 |
| 17     | <b>Integrity Pact</b> .....  | 41 |
| 18     | <b>Indemnity</b> .....   | 42 |
| 19     | <b>Security deposit by way of Performance Bank Guarantee</b> ..... | 43 |
| 20     | <b>Insurance</b> .....   | 43 |
| 21     | <b>Price Composition</b> .....                                     | 44 |
| 22     | <b>No Price Variations</b> .....                                   | 44 |
| 23     | <b>Import Obligations</b> .....                                    | 44 |
| 24     | <b>Term of execution of work</b> .....                             | 44 |
| 25     | <b>Confidentiality</b> .....                                       | 45 |
| 26     | <b>Settlement of disputes by Arbitration:</b> .....                | 45 |
| 27     | <b>Order cancellation</b> .....                                    | 46 |
| 28     | <b>Right to Accept or Reject the Quotation</b> .....               | 47 |
| 29     | <b>Right to alter quantities/components</b> .....                  | 47 |



**30 Force Majeure**..... 47

**31 Evaluation Process** ..... 48

    31.1 Technical Evaluation ..... 48

    31.2 Commercial:..... 48

    31.3 Formula for final evaluation..... 49

**Annexure I (RFP Download Declaration)** ..... 50

**Annexure II (Letter of Authorization)** ..... 51

**Annexure III (Organizational Profile)** ..... 52

**Annexure IV (Project List)**..... 54

**Annexure V (Black List)**..... 55

**Annexure – VI Forwarding Letter (Technical Bid)**..... 56

**Annexure VII (Technical Parameters)**..... 58

**Annexure VIII (Technical Approach & Methodology Document)** ..... 77

**Annexure – IX Forwarding Letter (Commercial Bid)**..... 78

**Annexure X (Commercial)**..... 79

**Annexure XI (PBG)**..... 82

**Annexure XII (EMD)**..... 85

**Annexure XIII (MAF)**..... 87

**Annexure XIV (Back to Back Support)**..... 88

**Annexure XV (Indemnity)**..... 89

**Annexure XVI (Confidentiality)**..... 91

**Annexure XVII (NDA)** ..... 93

**Annexure XVIII (Pre-Integrity Pact)**..... 96

**Annexure XIX (Reference Sites)** ..... 103

**Annexure XX (Detailed Specifications)** ..... 104

**Schedule – 1(List of Offices)** ..... 107

**Schedule – 2 (Location)** ..... 108

**Schedule – 3 (Existing Firewalls & UTMs)** ..... 108

**Schedule 4 (Calculation Table)**..... 109

**Document Check List**..... 110



## 1 Introduction

National Bank for Agriculture and Rural Development, a body corporate established under the NABARD Act, 1981 (hereinafter referred to as "NABARD") having its Head Office at Plot No. C-24, 'G' Block, Bandra-Kurla Complex, Bandra (East), Mumbai-400051 and Regional Offices and Training Establishments in different cities across the country, intends to invite sealed proposal from eligible Vendors/Bidders for Supply, Installation, Testing, Commissioning and Maintenance of Next Generation Firewall for NABARD's Data Center & Disaster Recovery Center.

## 2 Purpose of RFP

The purpose of this RFP is to invite techno-commercial bids from eligible vendors, for Supply, Installation, Configuration, Testing, Training, Commissioning and Maintenance of Next Generation Network Firewall and Creation of DMZ both in DC & DR fulfilling the functionalities as outlined in the **Annexure VII** of this document based on:

- Minimum Eligibility Criteria
- Technical bid
- Commercial bid

### 2.1 Information Provided

The Request for Proposal document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with NABARD. Neither NABARD nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

### 2.2 Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, NABARD and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RfP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of NABARD or any of its officers, employees, contractors, agents, or advisers.

### 2.3 Costs to be borne by bidder

All costs and expenses incurred by bidder in any way associated with the development, preparation and submission of responses including but not limited to; the attendance at meetings, discussions,

demonstrations, etc. and providing any additional information required by NABARD, will be borne entirely and exclusively by the bidder.

## 2.4 No Legal Relationship

No binding legal relationship will exist between any of the bidder and NABARD until execution of a contractual agreement.

## 2.5 Bidder's Obligation to Inform Itself

The bidder must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

## 2.6 Evaluation of Offers

Each bidder acknowledges and accepts that NABARD may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible vendor. The RFP document will not form part of any contract or arrangement, which may result from the issue of this document or any investigation or review, carried out by a bidder.

## 2.7 Errors and omissions

Each bidder should notify NABARD of any error, omission, or discrepancy found in this RFP document.

## 2.8 Acceptance of Terms & Conditions

A bidder will, by responding to NABARD for RFP, be deemed to have accepted all the terms indicated therein. A signed copy of the RFP should be submitted, as a token of acceptance of all the terms & conditions mentioned in the RFP.

## 2.9 Lodgment of RFP

### 2.9.1 RFP submission:

RFP document submission is required to be done as under:-

- i. The response to the present bid will be submitted in two parts, Technical Bid containing the General Terms and Conditions including compliance to Technical Specifications and the other one containing the Commercial Bid on or before **06 December 2017 at 1400 Hrs.** The bidder will have to submit the Technical Bid and Commercial Bid portion of the Bids separately.
- ii. Technical Bid should be submitted in sealed non-window envelope duly super scribing "**Ref No. NB.DIT/653/DIT-012-01/2017-18 dated 16 November 2017 - Bid for Supply, Installation, Testing, Commissioning and Maintenance of Next Generation Firewall - "Technical Bid"**". A soft copy should also be submitted in envelop. It should contain all the relevant information & annexures except Annexure IX & X.
- iii. Commercial Bid should be submitted in sealed non-window envelope duly super scribing "**Ref No. NB.DIT/653/DIT-012-01/2017-18 dated 16 November 2017 - Bid for Supply, Installation, Testing, Commissioning and Maintenance of Next Generation Firewall - "Commercial Bid"**". A

- soft copy should also be submitted in envelop.
- iv. Each page of the technical as well as commercial bid and any supplementary document attached, if any, should have the signature and the seal of an authorized person (having the authorization / power of attorney etc. to sign on behalf of the organization). The authorization should be given in the format given in **Annexure II**.
  - v. The price finalized shall remain valid for a period of **06 months** from the date of such finalization i.e, date of issue of PO. In case NABARD intends to avail additional products and/or services offered in response to this RFP on or before the expiry of 06 months, the same should be made available at the finalized rate.
  - vi. Technical Bid will also contain the bidder's information in the format as given in bid document.
  - vii. Technical Bid should **NOT** contain any pricing or commercial information at all.
  - viii. The detailed datasheet of the product must be furnished along with the Technical Bid.
  - ix. The bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person duly authorized to bind the bidder to the contract. The authorization shall be indicated by written power of attorney accompanying the bid. All pages of the bid except un-amended printed literature shall be initialed by the person or persons signing the Bid.
  - x. The bid shall contain no interlineations, erasures or over writing except as necessary to correct errors made by the bidder, in which case such corrections shall be initialed by the person or persons signing the bid.
  - xi. The bidder should quote the price for each item required by NABARD. The format for the same has been given in **Annexure X**.
  - xii. A signed copy of the RFP must be submitted along with the bid before the aforementioned closing date and time as mentioned in General Information Summary.
  - xiii. Any bid received by NABARD after the deadline for submission of bid prescribed by NABARD, will be rejected and/or returned unopened to the bidder, if bidder desires so.
  - xiv. Faxed/Emailed copies of any submission are not acceptable and will be rejected by NABARD.
  - xv. If the submission does not include all the required information and documents or is incomplete, the proposal is liable to be rejected.
  - xvi. All submissions, including any accompanying documents, will become the property of NABARD. Bidders shall be deemed to license, and grant all rights to NABARD to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other bidders and to disclose and/or use the contents of the submission as the basis for processing of RFP, notwithstanding any copyright or other intellectual property right that may subsist in the submission or accompanying documents.
  - xvii. At any time prior to the deadline for submission of bids, NABARD, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the Bidding documents by amendments.
  - xviii. Bidder may seek clarification in writing but not later than 10 days before close for bid submission date. Amendment will be notified by mails to all prospective Bidders, from whom NABARD has received the Bidding documents and will be binding on them. In order to provide, prospective Bidders, reasonable time to take the amendment into account in preparing their bid NABARD may, at its discretion, extend the dead line for submission of bids.

### 2.9.2 RFP Validity Period

The proposal must remain valid and open for evaluation for a period of at least 180 days from the last date of submission (or extended last date of submission) of RFP.

### 2.9.3 Queries regarding “Request for Proposal”

Bidders are required to direct all communications related to this RFP, at

**Chief General Manager,  
Department of Information Technology,  
Fifth Floor, C Wing, NABARD, Head Office,  
C-24, G-Block, Bandra - Kurla Complex  
Bandra (East), Mumbai 400051  
Contact Telephone Numbers (022) 2653 9671, 2653 9625  
Fax No. :(022) 26530087  
E-mail id : [dit@nabard.org](mailto:dit@nabard.org)**

NABARD will not answer any communication initiated by bidders later than 10 days prior to the due date for lodgment of RFP. However, NABARD may, in its absolute discretion, seek additional information or material from any bidders after the RFP closes and all such information and material provided must be taken to form part of that bidder's response. Bidders should provide details of their Fax, email and full address(s) to ensure that replies to RFP could be conveyed promptly.

If NABARD, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then NABARD reserves the right to communicate such response to all bidders. NABARD may, in its absolute discretion, engage in discussion or negotiation with any bidder (or simultaneously with more than one bidder) after the RFP closes to improve or clarify any response.

### 2.10 Notification

NABARD will notify all short-listed bidders in writing as soon as practicable about the outcome of their RFP. NABARD is not obliged to provide any reasons for any such acceptance or rejection.

### 2.11 Disqualification

Any form of canvassing/lobbying/influence/query regarding short listing, status, etc. will be a disqualification.

### 2.12 Definition

The following expressions hereunder and elsewhere in the RFP/Contract Documents used, unless repugnant to the subject or context thereof, shall have the following meanings hereunder respectively assigned to them:-

1. **NABARD** (also referred as Bank, purchaser) means National Bank for Agriculture and Rural Development, a body corporate established under the NABARD Act, 1981 (hereinafter referred to as “NABARD”) having its Head Office at Plot No. C-24, Block ‘G’, Bandra-Kurla Complex, Bandra (East), Mumbai-400051 and Regional Offices (ROs)/Training Establishments (TEs) in different cities across the country, shall include their successors and assignees for orders placed by NABARD.
2. **“RO”** means Regional Offices of NABARD
3. **“TEs”** means Training Establishments of NABARD
4. **“NGFW”** means Next Generation Firewall
5. **“WAF”** means Web Application Firewall
6. **“RFP”** means the bid document NABARD intends to issue, hereinafter called **Request For Proposal or RFP**, to the vendor, to participate in the bid for “NGFW Solution” as per scope of work, terms and conditions in this RFP.
7. **“Vendor”, “Successful Bidder”**: shall mean Individual, agency, Firm or Company selected by NABARD for the performance of the Contract and shall include its legal representatives, successors and permitted assigns.
8. **“SI”** stands for System Integrator.
9. **“OEM”** stands for Original Equipment Manufacturer.
10. **“Bidder”** shall mean any Person or Persons, Firm or Proprietor who participates in this Bid indicating his / her / their interest & offering the Project / Work and its successful completion.
11. **“Supplies”, “Project”, “Work”** mean specified job(s) and/ or work(s) of this RFP for delivery and installation of goods or services as mentioned in the RFP.
12. **“Complete”, “Completed”** (in the context of job(s) mentioned in this bid) wherever used to indicate completeness of the specified job(s) and/ or work(s) of the goods/services defined in the BoM & the Work Order. It shall be deemed as incomplete if any component of the BoM or of the WO are not supplied, delivered and installed, if supplied is not operational or not acceptable after acceptance testing in any respect.
13. The **“Contract”** shall mean the agreement between the parties as derived from the Contract Documents.
14. The **“Contractor”** is Same as Vendor.
15. **“ISP”** means Internet Service Provider.
16. **“EMD”, “Earnest Money Deposit”** i.e, Money (or equivalent) deposited along with, the bid indicating willingness to abide by the rules of the bid process and assuring NABARD the Vendor’s capability to take up the project and complete in stipulated time.
17. **“SD”, “Security Deposit”** i.e, Performance Bank Guarantee deposited with NABARD as a performance guarantee for the quality specifications of the NGFW Solution & and other services to be rendered during the warranty period.
18. **“Work order”** means Letter of intent given by NABARD to the successful bidder of the bid expressing interest and intention for entering into a contract with the successful bidder for carrying out the proposed job(s) mentioned in the bid.
19. **“TCO”** means Total Cost of Ownership i.e, total project cost
20. **“PO”** means Purchase Order i.e, Letter of intent given by NABARD to the successful bidder of the bid expressing interest and intention for entering into a contract with the successful bidder for carrying out the proposed job(s) mentioned in the bid.

21. **"Officer-in-charge"** shall primarily refer to the officer of NABARD to whom this bid is submitted, or any other officer within the same department who has been designated by him/her from time to time to handle the proceedings of this bid.
22. **"ECMS"** means Enterprise Content Management Solution.
23. **"HRMS"** means Human Resource Management System
24. **"CLMAS"** means Centralized Loan Accounting Management System
25. **"TALMS"** means Treasury Asset & Liability Management System
26. **"OSS"** means Off-site Surveillance
27. **"DCMS"** means Data Collector Management System
28. **"ILMS"** means Integrated Library Management System.
29. **"NABNET"** is the internal web portal of NABARD
30. **"Complete Agreement"**: The terms and conditions of the RFP along with work order shall constitute the entire agreement between the parties hereto. Changes will be binding only if the amendments are made in writing and signed by an authorized Official of NABARD and the Vendor. The start date shall commence on the 02<sup>nd</sup> (Second) day of work order or the date of acceptance, whichever is earlier.
31. **"Acceptance by NABARD"**: Authorized officer(s) of NABARD must certify & sign all the installation reports and the invoice(s) for the Bill of Material.
32. **"Downtime"** is the time between the Time of Report by NABARD and Time of Restoration/ resolution within the contracted hours.
33. **"Failure"** is the condition that renders NABARD unable to perform any of the defined functions on the ECM Solution.
34. **"Restoration"** is the condition when the vendor demonstrates that the ECM Solution is in working order and NABARD acknowledges the same.
35. **"TAMD"** means Technical Approach & Methodology Document.
36. **"Reverse Transition"** means the process by which successful bidder assists NABARD or its authorized vendor(s) to take up the entire support, maintenance etc operation for rendering desired services to NABARD.

### 2.13 Bid Currency

All prices shall be expressed in **Indian Rupees** only (Multiple of Tens only).

## 3 Background

### 3.1 About NABARD

National Bank for Agriculture and Rural Development, a body corporate established under the NABARD Act, 1981 ("NABARD") having its Head Office at Plot No. C-24, 'G' Block, Bandra-Kurla Complex, Bandra (East), Mumbai-400051 and Regional Offices and Training Establishments in different cities across the country. The mission of NABARD is to promote sustainable and equitable agriculture and rural prosperity through effective credit support, related services, institution development and other innovative initiatives. More details about NABARD, its products and services can be seen in the website "[www.nabard.org](http://www.nabard.org)".

## 3.2 Present IT set up

NABARD have standard LAN setup in its head office and all 33 Regional Offices/Training Establishments. All these offices are connected together in a WAN setup using a Multi-Protocol Label Switching (MPLS) backbone having a bandwidth of 2 Mbps for delivering various services.

NABARD has its Data Center (DC) in Mumbai and is built with Tier 3 Architecture with adequate redundancy in both Power and Data Network structure. The DC has adequate Rack/Server space for hosting the Firewall Solution.

NABARD has a Disaster Recovery Site opted in a co-location model near Delhi. The same MPLS-WAN network connectivity having 4 Mbps bandwidth is available for DC-DR communications.

NABARD has a DELL Chassis Module (M1000e) having a capacity of 16 Half Blade Servers (of which 4 blades (DELL M 620 Servers) have been populated. This server setup was put in place in April 2013 with a three years warranty.

NABARD has 2 UTM devices installed at each location including HO. These devices are in HA at each locations. There is Management & Log server at HO. Policy management is done centrally. Apart from the above a pair of Sonic Wall devices in HA are present at both DC & DR.

## 4 Scope of Work

### 4.1 Project Objective

In a bid to strengthen IT security of the Bank, NABARD intends to introduce Next Generation Enterprise Firewall having various security modules / components deployed in High Availability mode (replacing the existing SonicWALL firewall) at DC, introduce the same set of firewall at DR also and create DMZ in the network for internet facing applications at DC as well as DR. The objective of the exercise is the following:-

- “ The broad scope of work as detailed in this section refers to the hardware, software / licenses and services that is procured through this RFP and used for implementing the Next Generation Firewall at the primary Data Centre, Mumbai and Disaster Recovery Site near Delhi locations. In other words, NABARD intends to procure 4 nos. of appliance based Next Generation Firewalls System and get it installed by the successful bidder for detecting and stopping malicious traffic as a preventive control solution. The appliances must be implemented in HA at Mumbai and DR site near Delhi.
- “ Provision of all licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
- “ Ensure Installation, implementation & maintenance of the Firewalls as per NABARD's security architecture design & pattern of traffic.
- “ Comprehensive onsite warranty of 5 years for all the hardware/software under the project.

- “ Device rules / device policy definition and enforcement on the boxes proposed in this RFP.
- “ Enable to detect and block sophisticated attacks by enforcing security policies at various levels, prevent unauthorized access or malicious traffic within NABARD's system or in the network, ensure protection from zero day attacks and unknown threats.
- “ Enable NABARD to ensure that all the IT assets at DC as well as DR are secure from threats for today, tomorrow and in the future.
- “ A detailed design has to be chalked out along with the project plan in the form of TAMD document detailing but not limited to the indicated points as mentioned in Annexure VIII. The bidder shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the solution at NABARD's DC & DR.
- “ The bidder shall also handle all matters relating to the configuration and operation of the system including but not limited to application, system interfaces, documentation, user manual and training for the successful implementation of the system.
- “ The bidder shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by NABARD.
- “ The bidder should be responsible for de-commissioning of existing SonicWALL devices at DC i.e, replacing the existing SonicWALL at DC with the new firewall in such a way that there is no impact on business continuity. If need be, the successful vendor may arrange for resources with SonicWALL expertise to ensure the same.
- “ The bidder would ensure installation of the proposed appliance will include migration of policies and configuration of the existing SonicWALL (NSA4500) device at DC.
- “ The bidder should ensure that the entire activity of installation, commissioning & configuration whether done in a single pass or in Phases must be completed within 2 days (weekends) under all circumstance for each locations.
- “ The bidder is responsible for migration of existing rule base to the new devices, NATing, creation of rule base before go-live.
- “ The solution proposed should be compatible with the existing Checkpoint UTM firewall at DC and SonicWALL at DR.
- “ The solution implemented should have high availability features to ensure that systems will be available at any time of the day. The standby firewall (same make and model) being procured through this RFP for HA should be configured with all policy so that the same can be up when the primary one is down for any reason.
- “ Bidder should propose highly scalable enterprise class solution. Solutions with limited scalability would not be acceptable to NABARD. Solutions which are not mature for over 1 year should not be quoted.
- “ Introduce the proposed firewalls in the network to act as perimeter level firewall and allow the existing firewalls to function as core firewall both at DC & DR. Proposed firewalls need to be configured in such a way that they always function in tandem with the existing one towards achieving the goal of secure environment for the IT assets.
- “ Create DMZ to ensure that the critical corporate data remain protected from cyber threats.



- “ Install & configure management, reporting & logging tool to have a centralised and powerful management which should enable NABARD to deploy, view and control all firewall activity through a single pane. There should be an ability to automate routine tasks and drill-downs to produce maximum efficiency with minimal effort.
- “ Introduce two devices at each location in High Availability (HA) mode for business resiliency as well as business continuity.
- “ Both DC as well as DR should have identical perimeter security i.e, proposed firewalls should be identical in all respect for both the locations.
- “ Smooth & Knee-jerk free removal of the existing SonicWALL firewall from the DC network.
- “ Seamless Integration with existing security devices and tools present and future tools planned for procurement.
- “ The proposed firewalls should be able to perform the Link Aggregation function for connectivity from three or more ISPs
- “ Ability to integrate seamlessly with Active Directory, existing PIM tool to provide complete user identification and enable application based policy definition per user or group.
- “ Increase visibility and understanding of application traffic. Eliminate traffic control beyond allow / deny.
- “ Firewalls need to integrate more granular blocking capability as part of the base product and should go beyond port/protocol identification and move towards integrated service view of traffic rather than merely performing sheet metal integration.
- “ Enable to create granular security policy definitions per user and groups to identify, block or limit the usage.
- “ Provide application function control to identify, allow, block or limit usage of applications and features within them.
- “ Enable safe internet use while protecting against threats and malware. Scan for viruses and malware in allowed collaborative applications, protect environments with social media and internet applications.
- “ NABARD should have the power to create detailed policies that should be based on the characteristics such as user identity, user role and specific aspects of a web application. There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.
- “ Virtual Private Network (VPN) technologies should be part of the solution to provide resilient and flexible site-to-site, client to site connectivity. Should have management tools to deploy, configure and operate the VPNs.
- “ Identify and control applications sharing the same connection.
- “ Should be able to intercept, decrypt and re-encrypt SSL/TLS, SSH, and VPN traffic with low performance degradation.
- “ Decrypt outbound SSL traffic to ensure protection from sniffing etc..
- “ Enable the same application visibility and control for remote users.
- “ Deliver the same production throughput and performance with application control active.

- “ Updates and upgrades to remote sites should be automated and performed seamlessly with the ability to view and manage remote operations through the central management system.
- “ The product should have capability of deep packet inspection (DPI) to ensure various pieces of packet are thoroughly examined to identify malformed packets, errors, known attacks and other anomalies. It should rapidly identify and block Trojans, viruses, spam, intrusion attempts and other violation of normal protocol communications.
- “ Should have ability to manage security environment through intuitive graphical interface which should provide views, details and reports on security health through a comprehensive, centralised security dashboard.
- “ The user interface and system configuration of the management console should be comprehensive, flexible and easy to use such that it should be possible to exclude features that are needed in the enterprise environment.
- “ All the equipment (hardware, software) supplied as part of solution should be IPv6 ready from day one and should support all the protocols.

To summarize, NABARD is looking for following:-

| Sl.no. | Items  | Units | Location     | Remarks   |
|--------|--|-------|--------------|---|
| 1      | Next Generation Firewall (Hardware, softwares, licenses/ subscriptionetc.)               | 02    | DC           | Identical with the one proposed for DR                            |
| 2      | Next Generation Firewall (Hardware, softwares,licenses/subscriptionetc.)                 | 02    | DR           | Identical with the one for DC                                     |
| 3      | Management Server, Reporting & Log server(Hardware, softwares,licenses/subscriptionetc.) | 01    | DC           | Single pane / dashboard / tool to manage devices at both location |
| 4      | Warranty & Support for 5 years   | 01    | DC&DR        | 24x7 support  |
| 5      | On-Site Support for 01 year  | 01    | DC           | 8x5 support for both DC & DR but location is at DC                |
| 6      | Switches (L2)  | 02    | DC & DR each | If required   |
| 6      | Training   | 02    | Mumbai       | Admin Level training  |

## 4.2 Project Plan

Project Schedule: The bidder should provide a detailed project plan in terms of activity and phase wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of components for Next Generation Firewall Solution. The bidder shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation. The bidders shall provide a comprehensive Project Plan including Challenges, ways to

overcome those challenges, Quality, Migration, Conversion, Resource, Change Management Plan in the form of TAMD document. The bidder has to submit a detailed plan for migration and implementation of the solution. Plan should include the full scope of the project as mentioned above. On acceptance of such plan by NABARD, the vendor is required to carry out the implementation, migration and customization as applicable including supply, installation, and testing of solution etc. Bidder should be able to complete the project **within four (04) weeks** from the date of issue of PO under any circumstances. We intend to take up this project in a phased manner and follow the broad steps indicated below:-

1. SRS & Gap Analysis
2. Kick –Off
3. Development, Customization, Deployment & Installation
4. Testing
5. Go - Live
6. Training
7. AMC & Warranty

#### 4.2.1 SRS & Gap Analysis

The bidder/OEM must analyze the existing production system and gather performance metrics. The bidder/OEM should review firewall system parameters such as sessions, resources, and drops to verify that the firewall is performing optimally. Additional checks should review traffic, threat, and system logs to identify recommended changes as per best practices wherever applicable. The Bidder is also expected to provide suitable Business Continuity Planning applicable to the proposed solution in case the said solution is unavailable at any time or any site. The steps may be as follows:-

- Study of existing security architecture, existing firewall & IPS policies & propose enhanced security architecture as per best practice.
- Prepare migration plan for existing firewall & IPS policies along with Next Generation security features mentioned in technical specification.
- Give formal presentation to bank security team on final design, configuration and implementation based on TAMD document.
- All Design & configurations should be as per industry best practice of NGFW.
- Prepare a plan for all latest stable hot fix to be applied on NGFW
- Prepare the TAMD document and submit to NABARD.
- Get signoff for all User Acceptance Tests from Bank.

The Bidder will provide NABARD with the gap identification report along with the necessary solutions to overcome the gaps within the time limit and the time frames. The Bidder will incorporate all the suggestions made by NABARD to the gap report. The Bidder will also ensure that gaps pointed out by the audit and inspection team, statutory and regulatory bodies, or any other third party agency engaged by NABARD within the project period will be immediately resolved.

#### 4.2.2 Kick –off

After the TAMD document is shared by the vendor and approved by competent authority of NABARD the project would be considered to be ready for kick-off. The vendor is required to prepare a detailed project schedule & get it approved by competent authority of NABARD before kick-off.

#### 4.2.3 Deployment, Installation, Configuration

After the kick-off, the vendor would deploy, install, configure, test the proposed firewall and also decommission the existing SonicWALL firewall as per the project schedule. The Bidder must prepare architecture design, optimize network to increase performance, documentation, project plan and training as part of the implementation services.

#### 4.2.4 Testing

In the testing phase, all relevant tests need to be conducted as per the project schedule and satisfactory report should be obtained from the competent authorities of NABARD before preparing it for go-live. This report would be from all the stake holders i.e, HRMS, CLMAS, ENSURE, NABNET, ECM etc.

#### 4.2.5 Go-live

Post successful deployment, installation, configuration, testing of the system and after obtaining “Final System Acceptance” letter from the NABARD’s competent authority, the project would be considered as go-live.

#### 4.2.6 Training

Vendor is required to impart training to NABARD staff as per plan. Successful bidder should train the identified NABARD’s officials on the product which includes Central Console Management, log analysis, configuration i.e, Administrator level training at one of the OEM’s authorized center and by qualified trainer to enable the resource to carry out day-to day activity, administration, management, reporting and basic troubleshooting. Details of the training has been furnished in section 4.5.7.

#### 4.2.7 AMC & Warranty

When the system starts running, the vendor is required to sign SLA with NABARD.

Bidder is required to develop full system architecture to implement the proposed solution. The solution should have central management & log server for monitoring and control. The proposed solution should be implemented in such a way that there is no business impact on any of the existing applications such as HRMS, CLMAS, TALMS, OSS, ILMS, ECMS, DCMS etc.

To achieve the above objectives vendor is required to supply, commission, install/re-install, test, configure/re-configure and maintain & provide supports to the Systems in Data Centre at Mumbai, DR near Delhi. The bidder should have resources to independently decommission the existing SonicWALL firewall at DC from the network and introduce the propose solution in tandem with the existing Checkpoint at DC as well as existing SonicWALL at DR.

Bidder will have to specify the various infrastructure requirements which are to be provided for commissioning and smooth functioning of the equipment. This will include site requirements, power, cables, UPS, environmental conditions, illuminations etc. Details are given in section 4.5.3

**The broad Scope of Work (SoW) is as follows (However, NABARD reserves the right to modify SoW including any reduction or enhancement in the RFP to enable final selection of vendor for the project).**

**The deliverables of this project are following but not limited to:-**

### 4.3 Product Features

#### Essential:

- **Centralized Monitoring & Reporting** :-The proposed solution must have a separate management solution for management, logging and reporting to help NABARD in log analysis, policy management, firewall rules set export, rules & policy configuration and also to provide administrator with security health dashboard to view the happenings and traffic patterns and associated risks in network in real time. A centralized system should enable you to deploy, view and control all firewall activity through a single pane of glass. Central management should also give you the ability to automate routine tasks, reuse elements and employ shortcuts and drill-downs to produce maximum efficiency with minimal effort. It should include Web Based reporting, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. The reporting tool must ensure user friendly and customized report extraction, IPS, Web filter, Antivirus, Anti-spam system reports, IP and User basis report, various Compliance reports and reasonable no. of drilled down reports. Hardware to be quoted separately in case of external reporting solution.
- **User & Application Control**:- It should be able to identify, allow, block or limit applications regardless of port, protocol to provide visibility into unknown & proprietary application within NABARD's network. It should empower to create detailed policies that can be based on characteristics such as user identity, user role and specific aspects of a web application. It should have more advanced user and application controls such as the ability to expand user groups, domain names and TLS matches, as well as detailed user and application usage information in reports, logs and statistics.
- **Third-party identity management integration** : It should supports all major authentication protocols such as LDAP/AD, RADIUS, Kerberos and Local Authorization thereby helps organizations control not only the types of traffic that are allowed to enter and exit the network, but also what a specific user is allowed to send and receive.
- **Packet filtering** :- It should control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. It must support Identity awareness for granular control of applications by specific users, group of users and machines that the users are using.
- **Deep Packet Inspection**:-It should have the capability to examine the data part of a packet as it passes through it, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, log servers etc.. It must ensure the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies.

DPI can rapidly identify and then block Trojans, viruses, spam, intrusion attempts and any other violations of normal protocol communications.

- **IDS/IPS:** The device must have both inbuilt Intrusion Detection System and Intrusion Detection System. It may be either or all of the signature-based, statistical anomaly-based, and stateful protocol analysis. It must be able to detect and prevent the network efficiently from different kind attacks like TCP/IP attack, HTTP attack, email attack, FTP Attack, , DNS Attack, ICMP Attack, DOS and DDOS Attack, Telnet Attack. It should have enough signatures. IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection. The IPS capability shall minimally attain Internet Computer Security Association (ICSA).
- **TLS/SSL traffic inspection:** The proposed solution should be able to effectively monitor SSL and http tunneled traffic flows. In order to secure encrypted traffic the proposed NGFW must support all inbound and outbound SSL decryption capabilities to help NABARD identify and prevent threats and malware in encrypted network streams.
- **QoS/bandwidth management:** It should have application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Zone, Group, Firewall Rule, URL and Applications to prioritize network traffic by ensuring control of traffic flows on the network so that traffic does not exceed network capacity and thereby resulting in network congestion and also allows to allocate bandwidth for certain types of traffic and also for applications and users.
- **Link Aggregation:** The appliance proposed should have the capability for Link aggregation. The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth
- **Network- and port-address translation (NAT):** It should be capable of allowing NATing & PATing for various purposes as per the requirement. All the equipment (hardware, software) supplied as part of solution should be IPv6 ready from day one and should support all the protocols.
- **Virtual private network (VPN) :-** IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5, SHA1 Hash algorithms, IPsec NAT Transversal.
- **Antivirus Inspection & Anti Bot:** The NGFW should be able to protect the network from Virus, Worm and should have the ability of Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, Zero hour Virus outbreak protection. It should have inbuilt antivirus engine and be able to inspect https traffic on the fly for any infected file and also for protocols like HTTP, HTTPS, FTP, POP3, SMTP, SMB etc. It should also be capable of identifying malware coming from incoming file and malwares downloaded from internet
- **Stateful inspection:** Solution should track the connections from layer 2 to layer 7 to allow a lot more control and provide NABARD with the ability to have very granular policies.
- **High Availability:** It must have high availability feature i.e, Active-Active, Active-Passive as well as Cluster to provide resiliency to the business etc.
- **Integration with security devices:** The device should be able to seamlessly integrate with other standard security solutions such as SIEM tools, reporting tool, two factor authentication systems etc. with little or no modifications and thereby enhance the overall capability of security system. Configuration/integration for log correlation with standard SIEM tool like Arcsight, RSA, QRadar etc and syslog servers like Solarwinds etc.

- **Wireless** : Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported APs

#### **Good to have features:**

- **Web Filtering:** It should screen an incoming Web page to determine whether some or all of it should not be displayed to the user. This filter would check the origin or content of a Web page against a set of rules for the Web filter.
- **Advance Persistence Threat Solution** : Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
- **Sandboxing:** Solution should inspect executables and documents containing executable content including .exe, .com, .dll, .docx, rtx, etc , Should support dynamic malware behavior analysis run files in real environment
- **Load Balance:** For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.
- **Two Factor Authentication:** Solution should support option to integrate with Email/SMS/token based 2FA for Internal as well as VPN users authentication.

(N.B. Solution having good to features along with the essential features would be preferred.)

## 4.4 Hardware

### 4.4.1 Next Generation firewall:-

NABARD is looking to implement Next Generation Firewall (NGF) with an integrated solution of Application Intelligence and Control, IPS, URL filtering, Anti-bot, Anti-virus, Anti-spyware, Web reputation, Identity awareness and VPN(both IPsec and SSL). The firewall would be deployed in the DC as well as DR Site in active / active mode. NABARD already has Checkpoint UTM in the core, hence for perimeter firewall Banks intends to have different make firewall i.e. **Checkpoint & SonicWALL firewall should not be quoted.**

### 4.4.2 Management, Reporting & Logging H/w

Solution must offer separate appliance to store logs and reports. In-built reporting will not be considered as it impacts firewall performance. Separate appliance must offer at least 10TB storage space with RAID. It should show real-time traffic details. Reporting appliance should have Threat Detection Service which should do Network Event Correlation and highlight threats to security administrator

### 4.4.3 Switches

To implement the abovementioned solution if there is any requirement of L1 or L2 switch the same may also be delivered along with the firewall and to be indicated in the proposal. The price may be quoted in the field provided in the commercials. The warranty for the same should also be for 5 years.

#### 4.4.4 Miscellaneous

NABARD would provide only the rack space & power. In addition to the above if any miscellaneous material, if any, is required the same may be bundled in the solution. The price may be quoted in the field provided in the commercials. If there is any delay in executing the project because of any item/product other than rack space & power it will be sole responsibility of the successful bidder.

#### 4.5 Softwares

The proposed solution should be bundled all the softwares, firmwares, licences, subscriptions etc. Biudder should ensure that all licenses/subscriptions like appliance, management Server, Operating System, database (if required), up-gradation etc. are part of the offer. Any corruption in the software or media shall be rectified during the full period of the contract including Warranty and AMC, at no extra cost to the Bank. Software /Firmware updates and upgrades during period of warranty / AMC should be at no additional cost to Bank.

##### 4.5.1 Licenses/subscription

The solution offered should have all the licences / subscription for five years with warranty & support for the components offered. It must have licences for the components mentioned as Essential in the section 4.3.1. The cost of the components may be indicated in Annexure X.

##### 4.5.2 Operating System

The operating system loaded on the appliances should be latest & stable. Solution should have hardened OS for all appliances. Successful bidder should ensure that all the patches are updated from time to time during the entire contract (warranty, extended warranty & AMC as the case may be) without any extra cost to NABARD.

##### 4.5.3 Firmware

All the requisite firmwares should be part of the offer. Successful bidder should ensure that all the patches are updated for all the appliances from time to time during the entire contract period (warranty, extended warranty & AMC as the case may be) without any extra cost to NABARD.

##### 4.5.4 Database

If required, bidder may offer database for the system. Successful bidder should ensure that all the patches are updated for all the appliances from time to time during the entire contract period (warranty, extended warranty & AMC as the case may be) without any extra cost to NABARD.

##### 4.5.5 Miscellaneous

In addition to the above if any other software is required the bidder must include the same in the offer.



## 4.6 Services

### 4.6.1 Implementation of Firewalls

The vendor should ensure that the study of the existing architecture is properly done. Based on the study and the SRS the successful bidder would ensure the following:-

- i. The vendor is responsible for ensuring seamless integration of the proposed product/s, with Bank's existing security devices, network and applications. The vendor shall ensure that this happens as per the security policy and security architecture blueprint already defined by the Bank, the same may be shared on need basis with the selected vendor.
- ii. The vendor is responsible for installation and performance tuning. It should provide onsite support during the installation phase to assist with equipment setup, software installation and configuration, and performance tuning so that the solution operates as proposed on the production network.

### 4.6.2 Creation of DMZ in the existing network

The DMZ to be created should consider the following:-

- iii. Connections initiated from the inside interface toward the DMZ, and configure the firewall accordingly.
- iv. Connections initiated from the DMZ interface toward the outside, and configure the firewall accordingly.
- v. Connections initiated from the outside interface toward the DMZ, and configure the firewall accordingly.
- vi. Connections initiated from the DMZ interface toward the inside, and configure the firewall accordingly.
- vii. The DMZ created should allow all the traffic to internet facing application to pass smoothly i.e, HRMS,NABNET, DCMS,ECM, TLMAS and CLMAS application hosted in NABARD DC.
- viii. Vendor is responsible to replicate the same in DR.
- ix. The cost of all customization efforts is required to be included in the Price Bid and NABARD will not pay any additional cost for such effort.

### 4.6.3 Warranty, Extended Warranty, AMC & FMS

Successful bidder would enter into Service Level Agreement for Comprehensive Annual Maintenance Contract (AMC) & Facility Management Services (FMS) with NABARD to provide maintenance support to hardware equipment and software for warranty period of at least **05 years**. Bidder would also arrange for spare parts upto the period of 5 years warranty period or extended warranty period. During this period the vendor will ensure smooth functioning of system. Bidder shall provide warranty support/ AMC & FMS services for **24x7** with 1 hour response time besides uptime commitment as mentioned in the Uptime Efficiency.

Under warranty / AMC & FMS following services are required to be rendered by the bidder:-

- i. To maintain the software products & hardware at least for 5 years (warranty and post warranty).
- ii. The warranty/AMC should cover the support for Hardware, Software, firmware etc. under the project.

- iii. To provide on-site annual maintenance and support services for the implemented solution (Hardware & Software), if sought.
- iv. The Warranty & support charges for all components except the cost of the AMC engineers. The cost for one engineer should be given separately. NABARD reserves the right to ask for additional engineers, if need be, at the same cost.
- v. The bidder would be responsible to undertake On-Site support activities for a period of at least 01 year. The bidder must be ready to undertake AMC activities post expiry of the warranty or extended warranty period on mutually agreed terms & conditions.
- vi. In case need arise NABARD may seek AMC & FMS services post warranty & extended warranty period from the successful bidder. The cost of AMC should not be more than 20% of the average of Warranty cost averaged over five years.
- vii. The AMC for the hardware equipment would be awarded to the bidder at the rate as quoted as INR in the price bid. However the AMC services for the above mentioned equipment would be procured by the bidder solely from the OEM at SLA's matching those during warranty support (as mentioned in Section 4.6.12). The bidder has to agree that AMC rate will remain valid and unchanged during the AMC & FMS for entire contract period.
- viii. The AMC contract should cover the services which the supplier provided under warranty.
- ix. Warranty of the appliance with software will be for five year from the date of successful installation. It would be the vendor's responsibility to provide for the latest version/upgrades/hot fixes/patches and installation of the same etc. for the proposed solution, as and when they are released during the period of warranty, extended warranty /AMC period.
- x. Adequate number of qualified and OEM certified support engineers (at least two) should be provided for on-site support.
- xi. During the warranty period as well as comprehensive post warranty Annual Maintenance Contract period, vendor should ensure 99.5% uptime (calculated on a 24\*7 hour window on monthly basis) of the proposed solution. The calls should be attended to as per Service Level Agreement (SLA). This shall include hardware spares, Software, upgrades, patches, installation and service support. All defective parts must be replaced within 24 Hrs.
- xii. Provide on-site comprehensive support for the supplied items - equipment / systems / subsystems (hardware / software). Such support should include replacement of defective parts / equipment and / or repair of the same and must be considered within the scope of the project.
- xiii. Installation / re-installation / maintenance / reconfiguration of OS, system software and order supplied software.
- xiv. Components shall be replaced with a similar or better make and configuration.
- xv. All system patches, upgrades, service packs etc. of the OS and all other software supplied by the OEM must be made available free of cost.
- xvi. Support of integration and update of infrastructure / network configuration and change management of the entire solution (existing as well as that procured as scope of this tender) to meet business requirement.
- xvii. Any change in the IP scheme, if required, limited to all the equipment installed at Data Centre should be done in consultation with NABARD.
- xviii. Support should include policy & Rule base tuning to enhance the performance of the overall system and comply with SLA requirements on a continuous basis.
- xix. Security management of the system needs to be maintained at the expected service levels.

- xx. Monitoring and tracking performance and taking corrective actions to optimize the performance on a regular basis.
- xxi. Log storage management activities including regular backup, restore and archival activities.
- xxii. To provide support to system administrators in usage and management of the application.
- xxiii. Help Desk :-
  - a) The vendor shall use the existing Help Desk module of NABARD for providing support.
  - b) The vendor should provide at least two levels of service personnel as indicated above :
    - L1: Vendor's trained & qualified IT personnel stationed at NABARD's premises
    - L2: Vendors next escalation level etc.

NABARD reserves the right to cancel the AMC contract after giving 3 (three) months of notice. In case service provided under AMC is not satisfactory. In such case, NABARD shall execute an AMC contract with any other party for the balance period, at the risk and cost of the bidder. However, in case this situation arise bidder would actively carry out reverse transition process to the satisfaction NABARD.

#### 4.6.4 On-Site Support

Vendor will ensure availability of 01 (one) certified & trained manpower at NABARD's Data Centre for day-to- day activity and maintenance of the system at DC as well DR. Should the need arise successful bidder would arrange resources for DR site on need basis. The Bank reserves the right to conduct interviews of the proposed engineer. Prior to deployment of engineer, bidder has to forward complete bio-data along with certifications, if any. In case the engineer is not found suitable Bank may reject.

Following are the conditions:-

- i. The bidder to deploy engineer for a period of 01 year having experience of at least 2 years on proposed firewall technologies OR Professional Certified engineer on proposed firewall technology with 1 year post certification experience.
- ii. The engineer has to be deployed after completion of acceptance of solution by the bank and intimation to the bidder. The engineer would be operating from Banks.
- iii. The primary responsibility of the engineer would be tune the firewall, IPS, application control etc. based on the traffic history and also train the bank staff/engineers. The engineer should document and knowledge transfer to NABARD's officials.
- iv. The engineer should be present:
  - a) 8X5basis for a period of three months, Monday to Friday, excluding Saturdays, Sundays and national holidays.
  - b) The engineer should be present during normal Bank office hours at Mumbai i.e. from 9:00am to 5:00pm.
  - c) In case of exigencies or as and when Bank requires, the engineer should be available on Saturdays, Sundays and Holidays as well.

#### 4.6.5 Preventive Maintenance

- i. Periodic preventive maintenance of hardware, once in every quarter from the date of acceptance by the bidder during warranty /AMC period.
- ii. During the preventive maintenance the bidder should check the firmware / operating system running on the firewalls and other components and upgrade the same to latest version as released by OEM.

- iii. In case of release of any new version of OS or firmware it is responsibility of successful bidder to ensure that the upgradation is done proactively and without any extra cost to NABARD.

#### 4.6.6 End of Sale and End of Support

- i. The System spare parts/services, as and when required, and complete maintenance of the Systems during warranty / AMC period, shall be supported for a period not less than 7 years (including 1 year additional after expiry of warranty(including extended warranty)/ AMC, if required) from the date of acceptance of the System by the Bank.
- ii. The hardware supplied as part of this contract should not be declared End of Sale for period of 3 years from last date of submission of bids and should not be End of support for at least 3 years from thereon.
- iii. NABARD may be notified in writing, well in advance, about the End of Sale & End of Support so that the necessary action may be initiated without delay.

#### 4.6.7 Training

Bidder should provide training to NABARD's officials for using and managing the system which will include technical and administration training. Purpose of these training is to enable the officials to handle the day to day system operation. The bidder shall impart training to NABARD's identified IT personals (around 2 nos.) for the following areas at any of the OEM's authorized training institute :-

- i. Knowledge Transfer Training of the Deployed Solution Architecture and Design.
- ii. Enable them to perform day-to day activities i.e, framing rules & policies, extracting report etc.
- iii. Firewall platform Administration, Configuration & Management.
- iv. Basic level user level troubleshooting.

Necessary training infrastructure would be provided by the successful bidder and would be arranged at one of the OEM's authorized training center, preferably, in Mumbai. The bidder will have to ensure that training is imparted in a professional manner through Qualified Personnel and Course Materials would have to be provided for the same. An on-line / off-line self-learning mechanism should be available for all users to learn and use the product themselves.

### 4.7 Requirement

#### 4.7.1 Infrastructure

- i. All the activities / processes of the offered solution will be carried out at NABARD's premises. NABARD would provide the basic infrastructure in the premises with network, telephones, Fax, as required for providing solution for the processes.
- ii. The vendor should supply all necessary hardware/software for hosting the proposed solution and also to support all the software mentioned above.

#### 4.7.2 Software

- i. The proposed solution should include all the functionalities as prescribed in **Annexure VII**.
- ii. All the software modules of the proposed solution should be latest as well as stable one and must have a general release date prior to the date of the submission of the proposal.
- iii. None of the proposed solution shall be in alpha or beta version or unreleased as of the date of release of the bid proposal.
- iv. Vendor should supply management , logging & reporting tool
- v. Vendor should install, configure, test and integrate all of the various components of the solution
- vi. Supply, installation and maintenance of Operating System, Firmware and other tools if any.

#### 4.7.3 Hardware

- i. To supply, install and commission the Hardware. Details of the hardware are to be given in the **Annexure XX**.
- ii. Bidder to note that, Syslog server is already in place and Bank is in the process of setting up of SOC. The bidder to integrate the logs initially with syslog server and once banks SIEM is in place to integrate the logs to the same.
- iii. All the equipment (hardware, software) supplied as part of solution should be IPv6 ready from day one and should support all the protocols.
- iv. Identical arrangements have to be made by the bidder for DR also.
- v. Back to Back arrangement with OEM for all types of warranty & support for the entire project period plus AMC period including the extended AMC period. Bidder should submit the document in the format given in **Annexure XIV**.
- vi. The solution having high availability feature should be designed with no single point of failure and it should be hosted in a central location (Mumbai) and DR site near Delhi.

#### 4.7.4 Network requirements

Vendor has to indicate all the network level requirements such as:

- i. Bandwidth requirement at user level for the proposed firewall solution should be indicated.
- ii. Any specific network equipment like network level Load Balancer, accelerator etc. if required should be supplied as part of NGFW solution.

#### 4.7.5 Management, Reporting & logging module

Vendor should provide comprehensive Management reporting module (MIS) for the following purpose:

- i. Centralized management and reporting framework should be supplied as Hardware Appliance/Physical/Virtual Server
- ii. Centralized management and reporting and appliance should have capability of minimum 2 TB storage capacity with provision for future expansion and should support 10GB logs per day capacity
- iii. Any changes or commands issued by an authenticated user should be logged to a database.

- iv. Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.
- v. Role based administration with multiple administrators should be supported
- vi. Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.
- vii. All proposed components NGFW, Logging, Reporting etc should be managed from centralized management framework and if not then vendor need to provide additional components if any
- viii. Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc need to be provided with Real-Time and Historical reporting all the components.

#### 4.7.6 Licensing

- i. There shall not be any requirement for separate licenses for view only users.
- ii. No extra license fees /implementation charges should be charged by the selected bidder for implementing the solution at the Disaster Recovery site of NABARD.
- iii. Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided.
- iv. Licensing model should be device based.

#### 4.7.7 System & Security Audit

- i. Before live implementation of the solution in production system, the product may be audited by NABARD's appointed Security audit firm/in house team. All audit points raised by the Software Auditor should be complied with by the selected vendor without any extra charge. During warranty and AMC period vendor need to comply with security and system audit observation and remove the audit observation.
- ii. The solution should have built in security features to comply with the requirements of regulatory agencies.
- iii. It should have high level of reliability with particular emphasis on data integrity and security.
- iv. The system should generate industry standard logs and audit trails for managing and controlling the system. Logs & audit trails must be preserved for all the days from the day of Go-live for audit or forensic investigations.
- v. The system must be compliant to the IT Act 2000 and all other relevant Acts or Schedules.

#### 4.7.8 Testing

Vendor would assist NABARD in the following:-

- i. Functional tests to demonstrate that the each component as well as entire completed system performs the functions as is designed to function
- ii. Load tests to demonstrate the ability of the system to perform without performance degradation under maximum traffic load carrying conditions as defined in the OEM's specifications.
- iii. Performance tests to demonstrate satisfactory performance during the testing phase before Go-Live.

- iv. The vendor shall conduct the tests, rectify any problems and provide a fully operational & efficient system.
- v. UAT will be firstly done by the identified IT staff or any appointed agency or a third party, if NABARD desires so.
- vi. Vendor should provide an official signed document accepting the system (“Final Systems Acceptance”) from the NABARD’s authorized personnel.
- vii. All the required S/w and H/w for the purpose should be provided by the Vendor.

#### 4.7.9 Installation Certificate

On successful installation and configuration of individual components and the solution as a whole, the successful bidder shall submit the following as part of the commissioning:

- i. The Installation documentation of the entire solution.
- ii. Security scheme for entire solution.

NABARD will issue a Installation Certificate / sign-off on the submitted installation and commissioning note of all the Hardware & Software thereafter will be considered as successfully commissioned.

Delivery documents would comprise of the followings:-

- Software: Following checks will be carried out for acceptance and the vendor will have to provide these details to the Bank in writing-
  - ✓ Media under this RFP should be defect free
  - ✓ Licenses / keys of the product
    - Paper
    - Softcopy
  - ✓ Product on the media should be of latest version
  - ✓ Software subscriptions and upgrades for the baseline period of warranty period.
  - ✓ Documentation and manuals
  - ✓ Any other material which needs to be provided.
- Hardwares: Following checks will be carried out for acceptance and the vendor will have to provide these details to The Bank in writing-
  - ✓ Appliance box / chassis
  - ✓ Interfaces cards with connecting cables
  - ✓ Operating software media
  - ✓ License
    - Soft copy
  - ✓ Manuals and documentation
    - Soft copy
  - ✓ Console cables
  - ✓ Power supply/ Power cord
  - ✓ Equipment should pass the Power On Self Test

#### 4.7.10 Final Acceptance Certificate

Final Acceptance certificate for the above mentioned activities shall be issued within one month after successful issue of installation certificate and fulfilment of statutory requirements where performance has been established in an integrated manner in normal operations and successful completion of Training to NABARD personnel. Bidder has no other obligation under agreement.

Warranty of the Hardware will start from the date of issue of Installation Certificate.

#### 4.7.11 Go – live

- i. The system is said to be go –live if after all the required components of Next Generation Firewalls are delivered, installed, commissioned, configured, rules are migrated and/or mapped wherever required, tested both at DC as well as DR, creation of DMZ, and entire components of the system are smoothly running as per the expectation of NABARD and issuance of Final Acceptance certificate/letter from NABARD's competent authority.
- ii. The date of Final Acceptance Certificate/letter will be considered as go-live date.

#### 4.7.12 AMC, Warranty & Support

- i. The products shall be under a warranty of minimum **five (05) years** during which additions/modifications/bug fixing/security objections shall be done without any extra charge. Further all upgrades, patches would be provided free of cost during the warranty period.
- ii. On-site, comprehensive Warranty BACK-TO-BACK from OEM for a period of 5 years from the date of acceptance.
- iii. AMC, if sought, will start after completion of warranty period.
- iv. Warranty for hardware and software components shall start from date of deployment of the respective components.
- v. However, in case warranty is not available from OEM, then it is responsibility of bidder to obtain annual technical support for the warranty year.

#### 4.7.13 Documentation and User Manual

Vendor should provide the following:

- i. Submit the detail (As Is and To Be) /system requirement specification document before kick-off of the project. This document should be approved and accepted by NABARD before commencement of the project.
- ii. Gap Analysis document before the kick-off stage.
- iii. TAMD document.
- iv. Detailed implementation schedule (module-wise) for entire solution has to be prepared and submitted.
- v. Delivery challan duly signed and dated by bank officials
- vi. Installation Report duly signed and dated by Bank officials. It should also have snap shots of step by step procedure followed.
- vii. Detailed Implementation document.
- viii. Vendor is required to submit weekly status reports showing progress against plan.
- ix. Complete user manual and system documentation (soft and hard copies) of the proposed solution after the go-live.
- x. Software version management and software documentation management reflecting features and functionality of the solution.
- xi. Copies of back to back warranty and support from OEM, licenses, all the credentials etc



- xii. Vendor should also provide other documents such as :
  - a. Screenshots of installation steps
  - b. Hard copy of the licenses, if any
  - c. Documentation for the processes implemented
  - d. Providing operational manual for products commissioned.

#### 4.7.14 Shifting of premise

- xiii. The Bank may, during the currency of the warranty/AMC, shift the equipment to other location(s) within the Country. The bidder needs to ensure that the OEMs and bidders warranty / AMC and support is valid across India. Further, bidder undertakes to continue to provide warranty/AMC and maintain/support the goods at the new location.
- xiv. Bidder will be informed about old and new location/office details as and when the Bank decides to shift the hardware due to operational requirements. Bidder will deploy resource(s) for decommissioning of respective equipment at old location and Commissioning of equipment at new location at no additional cost.
- xv. The vendor is required to update their database and provide support, Warranty/AMC etc, for the shifted devices at the new location.
- xvi. The bidder should also provide support for un-mounting and mounting of firewall and other components from the rack in the event of reallocation of racks or changes made in DR site based on Banks requirements.
- xvii. The charges towards packing, physical shifting and insurance would be borne by the Bank whereas all the arrangements have to be done by the vendor. No additional cost whatsoever would be paid by the Bank for all the above activities.

#### 4.7.15 Others

Apart from Supply, deployment and implementation of a System following activities are integral part of the project without which project would not be deemed to be complete:-

- i. In case any functionality/feature which is being provided by third party, it must be compatible with all the modules/hardware. And the responsibility of integration of the same lies with the bidder.
- ii. Go-Live and Post-Implementation Hand holding Support for at least a week.
- iii. Vendor is required to give all sorts of support required in case NABARD decides to replace the solution with other solution in future or add any other security related device or implement SoC solutions (Logistics, Technical, Integration support etc.) without extra cost.
- iv. The vendor must also include a detailed resource plan that describes the Project Management and identify Implementation Teams' composition. It shall define the roles and responsibilities of each member and the number of man-days that will be required of each member.
- v. Business Process Reengineering – The vendor shall include the impact of the new system to the operations of NABARD. If applicable, the proponent shall recommend changes to the existing processes that would benefit NABARD.

#### 4.7.16 NABARD's Responsibility

It would be limited to the following:

- i. Make available site for installation with power, rack space, earthing, internal cabling (fiber / UTP) and patch chords/panels (fiber, UTP).
- ii. Provide complete details for configuring management IP, SNMP string etc.
- iii. Provide details of contact person at the location/office who would be coordinating during installation.
- iv. Providing downtime for installation / preventive maintenance of hardware items (Not more than 2 days per site).
- v. The vendor should communicate at least one week in advance, the proposed date for installation / preventive maintenance etc, based on which downtime would be obtained from the locations/offices.
- vi. NABARD or its outsourced vendor (ITSM team) from central location would be logging all calls with the vendor central help desk and coordinating for call closure.

## 5 Pricing

- i. All the prices should be given in the format given in **Annexure X**.
- ii. The prices stated, shall remain valid for 06 months after the finalization of the price i.e, from date of issue of work order.
- iii. No adjustment of the contract price shall be made on account of variation of costs of labour and materials or any other cost component affecting the total cost in fulfilling the obligations under the contract.
- iv. The price would be inclusive of all applicable taxes under the Indian law. However, payment towards taxes would be made at actuals.
- v. NABARD may give orders for additional items/services at the same price anytime within the contracted period.
- vi. The price bid should be completed as per the price bid format.
- vii. The Basic price must take into account all incidental costs associated with the provision of services including travel, transportation, communications, fees, etc. imposed on the bidder in India or any other country.
- viii. The prices once offered must remain firm and must not be subject to escalation for any reason within the period of validity. The entire benefits/advantages, arising out of fall in prices, taxes, duties or any other reason must be passed on to NABARD.
- ix. Any reduction in prices due to the vendor reducing the prices, reduction in duties, taxes etc., by the Government, shall be passed on to NABARD during the validity period.

## 6 Payment

No advance payment will be made along with the Purchase order under any circumstances. Payments towards the solution will be made in a phased manner as indicated below:

- Hardware

10% of the Hardware cost will be paid on acceptance of project plan by NABARD.

50% of the hardware cost on delivery and successful installation & testing.  
40% after one month from the go-live at both DC & DR.

- Implementation/installation Cost:-
  - 65% payment after successful installation.
  - 35% after one month from the go-live at both DC & DR.
- Warranty, AMC & FMS Services:-
  - a) This payment will be on quarterly basis.
  - b) Warranty, AMC charges towards support services and other service, if any, will be paid on quarterly basis during the warranty, AMC period after seeking the service.
  - c) Payment towards On-site support would also be paid on quarterly basis.

## 7 Eligibility Criteria

Offers are invited only from those Vendors/Bidders who fulfill the following eligibility criteria.

### 7.1 Technical

- i. The bidder must preferably be ISO 9001:2008, ISO 27001:2005 certified company.
- ii. The bidders must have office registered in India for at least five years. The bidder should submit the valid Trade License Certificate along with the Technical bid.
- iii. The bidder should be in existence in India and providing IT Security services/ business (i.e. preferably in the area of implementation of Firewalls/ UTM/IPS) for a minimum of three year as on date of RFP. (Please submit proof, such as Registration Certificate etc for existence and purchase order/work order showing implementation since last three years.)
- iv. The vendor/bidder must be Tier-1 (Platinum/Gold) partner of proposed OEM (Original Equipment Manufacturer).
- v. The bidder should be able to provide services at Mumbai & Delhi. The bidder should have presence with dedicated teams/ support available at abovementioned centers. Vendor may have support center near Delhi location. In case there is no support center at Delhi, vendor may be ready to provide support at their own cost. No travel, fooding, lodging etc. expenses would be paid by NABARD. There is no provision of remote support wrt these devices except for OEM's support. NABARD will not bear any expenditure for such arrangements.
- vi. The OEM OR THE Bidder should be in the business of firewalls in India for atleast five (5) years as on date of this RFP
- vii. Bidder must have experience in executing at least two similar project within last 03 (Three) years.
- viii. The bidder should be direct channel partner of the OEM, preferably highest level channel partner and should be the one point contact for the entire project.
- ix. The products offered preferably have been implemented in at least 2 banking/financial institutions in India of which one should be a scheduled commercial bank. These installations should be live at least for last one year.
- x. The products should appear in latest **Challenger or Leader's Gartner's Magic quadrant**. Bidder should confirm in their letterhead that offered solution against this RFP is from Challenger or Leader's quadrant of Gartner's report for 'Magic Quadrant for Enterprise Network Firewall'. Bidder need to submit latest Gartner Magic quadrant report for the same. Consistent presence in the Leader's quadrant for last three years would be preferred.

- xi. EAL4 certification would be preferred.
- xii. The bidder should provide proper authentication from the manufacturer/OEM as per the format given in **Annexure XIII** of the RFP. Bids without proper authentication from the manufacturer/OEM shall be treated as incomplete and shall be rejected.
- xiii. The bidder should have a dedicated comprehensive support service center at Mumbai having minimum 02 OEM certified engineers for each products. The engineers should have minimum 2 years working experience on the offered OEM or devices. In addition to the above bidder should have resources capable of decommissioning the existing SonicWALL at DC independently without support of SonicWALL and commissioning the proposed solution smoothly so as to ensure there is no impact on Business Continuity for more than 01 day under any circumstances. Details must be given in the table given in **Annexure III**. Documents in support of the same must be submitted.
- xiv. The Vendor/Bidder should not have been blacklisted by any Central/State Government Organization or PSU for any corrupt and fraudulent practice. An Undertaking by the Authorized Signatory on the letter head of the Vendor/Bidder should be submitted as a part of Technical Offer in format given in **Annexure V**.
- xv. All the employees/operator deployed by the vendor for the digitization activity must comply with government's rules and regulations like Minimum Wages Act, Provident fund and ESI facility standard.

## 7.2 Financial:

- i. Bidder should be a well-established vendor registered (existing for minimum 5 years) as a company under Indian Companies Act, 1956 or Companies Act 2013 and must have a valid Provident Fund Registration Certificate, GSTIN and Income Tax PAN.
- ii. Bidder should have minimum annual turnover of ₹.5 Crore in each of financial year i.e FY2016-17, FY2015-16 & FY2014-15.
- iii. Bidder should have total turnover of ₹. 1 Crore or more through similar projects i.e, implementation of security solution in the last three years. Supporting documents in this regard should be provided as a part of Technical offer.
- iv. The bidder must have registered net profit during last 3 financial years i.e 2014-15, 2015-16 & 2016-17. This should be individual company's turn over and net profit and not that of group of companies. Documents supporting Financial Statement (like Copies of published Annual Reports etc.) should also be supplied along with Technical offer.
- v. The bidder must have completed minimum two such Projects with project cost not less than ₹. 50 lakhs involving security solutions in last five years. Supporting documents in this regard should be provided as a part of Technical offer.
- vi. The Vendor/Bidder should submit its Organizational / Financial profile in the format given in **Annexure III** as a part of Technical Offer.

*(N.B. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made wrt Technical & Financial eligible criteria. NABARD reserves the right to verify /evaluate the claims made by the Vendor/Bidder independently. Noncompliance of any of the criteria will entail rejection of the order.)*

## 8 Signatory

- i. Bidders shall indicate the authorized signatories who can discuss and correspond with NABARD, with regard to the obligations under the Contract.
- ii. The bidder shall furnish proof of signature identification for above purposes as required by NABARD.
- iii. The letter in the format given in **Annexure II** must be submitted along with Technical Bid.
- iv. The successful bidder shall submit at the time of signing the contract, a certified copy of the resolution of their Board, authenticated by Company Secretary / proprietor, authorizing an official or officials of the company to discuss, sign agreements/contracts with NABARD , raise invoice and accept payments and also to correspond.

## 9 Amendments of bidding documents

NABARD may at its sole discretion amend the Bidding Documents at any time prior to the deadline for submission of bids. However in case of such amendment, the bid submission date may be extended at the discretion of NABARD. Amendments made prior to submission of bid will be provided in the form of Corrigendum to the Bidding Documents and will be issued and uploaded in the web-site only.

## 10 Pre-Bid Meeting

A pre-bid briefing meeting of the intending Vendors/Bidders will be held on **24 November 2017 at 1400 hours** at DIT, NABARD, BKC,Mumbai to clarify any point/doubt raised by them in respect of the RFP. No separate communication will be sent for this meeting. All communication regarding points requiring clarifications shall be given in writing to The CGM, DIT, NABARD,Mumbai by the intending Vendors/Bidders on before **1100 hours on 22 November 2017**. No request for change in date of pre-bid meeting will be entertained. After pre-bid meeting any deviations in the RFP, if any and clarifications, if any, will be published on NABARD's website on or before **27 November 2017 at 1500 Hrs**. No fresh queries would be entertained after pre-bidding meeting.

## 11 Opening of Quotation

- i. NABARD will follow two steps evaluation process for evaluation:-
  - a. In the first stage, only Technical Bid will be opened and evaluated. Those bidders satisfying the technical requirements as determined by the NABARD and accepting the terms and conditions of this document shall be short-listed.
  - b. In the second stage, the Commercial Bid of only short-listed bidders will be opened.
- ii. Technical bid will be opened on **06 December 2017 at 1430 Hrs**. However, the date & time of opening of the Commercial Bid would be notified after the technical evaluation process is over.
- iii. To assist in the examination, evaluation and comparison of bids NABARD may, at its discretion, ask the Bidder for a clarification of its Bid. The request for clarification and the response shall be

in writing and no change in the price or substance of the bid shall be sought for, offered or permitted.

- iv. NABARD will examine the bids to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed and whether the bids are generally in order.
- v. NABARD, at its discretion, may waive any minor infirmity or nonconformity or irregularity in a Bid, which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder. This shall be binding on all bidders and NABARD reserves the rights for such waivers.
- vi. The lowest Vendor/Bidder shall be selected on the basis of Technical Bid & Commercial Bid evaluation for award of the work. Detailed evaluation process has been explained in Section 26 of this document. However, NABARD is not bound to accept the lowest or any bid received.

## 12 Earnest Money Deposit (EMD)

- i. The Vendor/Bidder shall furnish an EMD for an amount of ₹. 1.00 Lakh (Rupees One Lakh only) in the form of Bank Guarantee/ Demand Draft / Pay Order drawn in favor of National NABARD for Agriculture and Rural Development, payable / enforceable at Mumbai.
- ii. The Bank Guarantee in lieu of EMD should be given as per the format given in **Annexure XII**.
- iii. The EMD of unsuccessful Vendors/Bidders shall be returned within reasonable period, only after the successful completion of the Bid Process. No interest is payable on such amount.
- iv. The EMD of successful Vendor/Bidder will be returned only upon submission of PBG by the successful vendor or Issue of Final Acceptance Letter by NABARD whichever is later. No interest would be payable on this amount.

### 12.1 The EMD shall be forfeited if

- i. Vendor/Bidder withdraws his offer during the period of validity of the bid.
- ii. Non-acceptance of the orders when placed or Non-confirmation of acceptance of orders within the stipulated time after placement of orders. In case the successful bidder fails to duly acknowledge the acceptance of work order within the stipulated time of **02 days** from the date of issuance of work order, the EMD of the successful bidder may be forfeited without any further communication to the successful bidder.
- iii. The successful bidder should start working on the project within **02 days** of the acceptance of the work order failing which NABARD reserve the right to forfeit EMD amount from the successful bidder.
- iv. Any unilateral revision made by the Vendor during the validity period of the offer.
- v. If the successful Vendor/Bidder fails to execute the project satisfactorily within the stipulated time schedule.
- vi. NABARD's decision in the above cases will be final.

## 13 Performance

The Bidder will be bound by the following SLA during the warranty period of the material supplied as well as during the post warranty/ AMC period:-



### 13.1 Uptime Efficiency

The bidder shall guarantee an uptime of **99.9%** for all the locations where the system is installed & configured during warranty, extended warranty period and also during AMC, if contracted, which shall be calculated on monthly basis.

- i. The Downtime calculated shall not include any:
  - a) Failure attributed to NABARD (Power, Network etc.)
  - b) Preventive maintenance activity and
  - c) Force Majeure.
- ii. However bidder shall inform NABARD 7 days in advance before doing preventive maintenance or pre-planned activity.
- iii. Successful vendor shall provide 24x7 service support by deputing their engineer as and when required.
- iv. Vendor shall ensure delivery of any replacement/repair of damaged part or equipment within same day from the time of reporting at no extra cost to the Bank.
- v. The percentage uptime is calculated on **monthly basis (24 hours a day)**.
- vi. If the bidder fails to maintain guaranteed uptime of 99.9%, NABARD shall impose penalty as mentioned below on slab.
- vii. The performance would be measured as under on monthly basis:

$$\text{Performance (\%)} = \frac{\text{(Total contracted minutes per month – downtime Minutes within contracted minutes per month)}}{\text{Total contracted minutes in a month}} \times 100$$

viii. Amount of penalty to be calculated on monthly basis for the shortfall in performance compliance level is as under :

| Sl.No. | Shortfall in Performance | Penalty(% of the contract value of the services) |
|--------|--------------------------|--|
| 1      | <= 1%                    | 1  |
| 2      | >1% and <= 3%            | 3  |
| 3      | >3% and <= 5%            | 5  |
| 4      | >5% and <=6%             | 6  |
| 5      | >6% and <=8%             | 8  |
| 6      | >8% and <=10%            | 10   |
| 7      | More than 10%            | 25   |

ix. The above penalty shall be applied for each location separately.

The amount of penalty would be adjusted while releasing the Performance Bank Guarantee by extending the warranty/AMC period for the hardware accordingly.

### 13.2 Response Time to errors

The NABARD will classify all errors in to two categories: Critical & Low level errors.

- i. Critical errors defined as the Errors that require/cause NABARD to shut down firewalls.
- ii. Low Level Errors defined as those other errors that are not the Critical errors as defined above.

- iii. In case of an occurrence of an error in the system, NABARD reserves the sole right to categories it under one of the above category. The decision taken on this regard by NABARD shall be final and binding on the vendor.
- iv. The vendor should undertake and guarantees that all the Critical Errors will be resolved within one hours of the NABARD intimating the same through e-mail, telephone or fax.
- v. In case the Critical Errors are not resolved within the stipulated time as above, there shall be a per day penalty of 1% of the warranty & support cost per year for every day exceeding above said 4 hours resolution time apart from replacement of the respective hardware/software at Vendor's own cost for solving the errors. Such penalty shall be adjusted as maintenance credit against the AMC/Warranty cost payable by the NABARD to the vendor.
- vi. The vendor should undertake and guarantees that all the Low Level Errors will be resolved within 4 hours of the NABARD intimating the same through writing, telephone or fax. In case the Low Level Errors are not resolved within the stipulated time as above, there shall be a penalty of 1% of the warranty & support cost per year for every four (4) day's delay in resolution time apart from replacement of the respective hardware/software at the Vendor's own cost for solving such errors. Such penalty shall be adjusted as maintenance credit against the AMC charges payable by NABARD to the vendor.
- vii. Successful vendor shall provide 24x7 service support by deputing their engineer as and when required.
- viii. All defective parts must be replaced within 24 Hrs from the time error is reported.

## 14 Spare parts

The vendor is required to provide or arrange to provide all the spare parts till the expiry of Warranty, extended warranty or AMC/ATS contract whichever is later. Bidder should submit the Back to Back warranty certificate from the respective OEMs. All defective parts must be replaced within 24 Hrs.

## 15 Ethical Standard

Bidders are expected to observe the highest standard of ethics during the procurement and execution of this Contract. In pursuit of this policy, NABARD will reject a proposal for award if it determines that the Bidder being considered for award has engaged in corrupt or fraudulent practices in competing for the Contract. For the purposes of this provision, the terms set forth below are defined as follows:

- (i) "*corrupt practice*" means the offering, giving, receiving, or soliciting of anything of value to influence the action in the procurement process or in Contract execution; and
- (ii) "*fraudulent practice*" means a misrepresentation of facts in order to influence the procurement process;
- (iii) "*collusive practice*" means designs to establish bid prices at artificial, non-competitive levels to deprive BL of the benefits of competition.

By signing the Bid-form the Bidder represents that for the hardware it supplies, it is either the OEM or that it has proper authorization and/or license from the owner to offer them. Wilful misrepresentation



of these facts shall be considered a fraudulent practice without prejudice to other remedies that NABARD may take.

## 16 Information Security

1. The Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, storage tapes or any other media out of NABARD's premise without written permission from NABARD.
2. The Bidder's personnel shall follow NABARD's information security policy and instructions in this behalf.
3. Bidder acknowledges that NABARD's business data and other NABARD proprietary information or materials, whether developed by NABARD or being used by NABARD pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to NABARD; and Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Bidder to protect its own proprietary information. Bidder recognizes that the goodwill of NABARD depends, among other things, upon Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder could damage NABARD. By reason of Bidder's duties and obligations hereunder, Bidder may come into possession of such proprietary information, even though Bidder does not take any direct part in or furnish the Services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by this Contract. Bidder shall use such information only for the purpose of performing the Services.

Bidder shall, upon termination of this Contract for any reason, or upon demand by NABARD, whichever is earliest, return any and all information provided to Bidder by NABARD, including any copies or reproductions, both hardcopy and electronic.

## 17 Integrity Pact

As per Central Vigilance Commission guidelines, all PSBs/Insurance Companies/Financial Institutions shall implement Integrity Pact (IP) in respect of all major procurements, which essentially envisages an agreement between the prospective vendors / bidders and the buyer (i.e. NABARD), committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. It is a written agreement between the buyer and all bidders and stipulates rights and obligations to the effect that neither side will pay, offer, demand or accept bribes; collude with competitors to obtain the contract; or engage in such abuses while executing the contract. The purpose of the Pact is to make the procurement and contracting process fair and transparent. A proforma of the same is furnished in **Annexure XVIII**. The Prospective vendors have to submit the same duly signed on a non-judicial stamp paper of Rs.100/- at the time of submission of the RFP document.

The IP also envisages appointment of Independent External Monitors (IEMs), persons having high integrity and reputations, who will examine any complaint received regarding tenders and submit their report to the Chief Executive and also to the CVO in case of suspicion of irregularities. A format for the complaint to be recorded is enclosed to the proforma of the Integrity Pact.

## 18 Indemnity

The Vendor/Bidder shall indemnify NABARD against all claims in respect of patent rights, design, trademarks of name or other protected rights in respect any hardware and/or software used for Firewall Solution or in connection with the works or temporary works and from against all claims, demands proceedings, damages, costs, charges and expenses whatsoever in respect thereof or in relation thereto. The Vendor/Bidder shall defend all actions arising from such claims, before any such infringement and receive their permission to proceed, and shall himself pay all royalties, license fees, damages, costs and charges of all and every sort that may be legally incurred in respect thereof including third party claims. The vendor /Bidder shall be responsible for the loss or damage to the data and shall indemnify for the same. The successful Vendor/Bidder is required to submit a “letter of indemnity and undertaking” as per the prescribed format **Annexure XV** within thirty (30) days of commissioning of Firewalls.

- (a) It is clarified that the bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to NABARD's (and/or its customers, users and service providers) rights, interest and reputation.
- (b) Bidder shall be responsible for any loss of data, loss of life, etc, due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc, as such liabilities pose significant risk.
- (c) Bidder should take full responsibility for its and its employee's actions. Further, since NABARD's data could be integrated/used under Bidder provided software, the Bidder should be responsible for loss/compromise or damage to NABARD's data.
- (d) In the event that NABARD is called as a defendant for IPR infringement of patent, trademark or industrial design rights arising from use of any of the components of the supplied solution, the Bidder on its own expense, will undertake to defend NABARD.
- (e) It will be the Bidder's responsibility to rapidly do away with such third-party claims. The Bidder will also pay any compensation arising from the infringement claims and NABARD will in no manner be responsible for such payments. In addition, the Bidder will bear all the related expenses and legal fees.
- (f) On its part, NABARD will immediately relay to the Bidder any such claims and offer assistance within reasonable limits to rid the claim.
- (g) The Bidder must undertake to indemnify that all the components delivered are free of defects, are brand new and original. If at some stage it is discovered that the components do not meet these criteria, NABARD has the right to cancel the order and the Bidder will have to refund the total amount received from NABARD along with the interest and separate penalties. Similar conditions apply to software as well the system software must be licensed and original.
- (h) Bidder shall indemnify, keep indemnified, hold harmless, defend and protect NABARD and its employees/ officers/ staff/ personnel/ representatives/ agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all

other statutory obligations arising there from.

## 19 Security deposit by way of Performance Bank Guarantee

- i. The Vendor/Bidder guarantees that he shall repair or replace free of cost, equipment, machinery, its parts and components found defective on account of bad workmanship or defective materials or inferior manufacture as mentioned in the warranty and guarantee clauses. The successful Vendor/Bidder should provide a performance bank guarantee for a period of 05 (Five) years for an amount equivalent to **10% of the total order value** of hardware and software from a Scheduled Commercial Bank in the format specified by NABARD within 30 days from the date of Work Contract. The Proforma for Performance Bank Guarantee is attached as **Annexure XI**. In the event of the Vendor failing to make and maintain a security deposit in the manner aforesaid, the vendor shall be liable for forfeiture of the EMD money with NABARD submitted by them and NABARD shall be entitled to cancel the work order.
- ii. In case, the Vendor/Bidder does not perform under the contract to the full satisfaction of NABARD, NABARD reserves the right to reject the items / services rendered under the contract in its entirety or partially, as the case may be, during the evaluation period and Vendor/Bidder shall be liable to refund the full or proportionate amount, if already paid for the said items / services etc. In this regard the decision of NABARD shall be final. The guarantee will be valid till the expiry of warranty period (extended warranty) and AMC period i.e., **five years**.
- iii. Any deficiency or deficiencies observed by NABARD during the warranty period or before, in the performance or quality of the Firewalls & its functioning or services rendered can separately or collectively be subject to deduction of sums as compensation from the Performance Bank Guarantee (PBG) deposited with NABARD to a value as per the clause 15(i) above.
- iv. The NABARD shall be entitled to deduct from the deposit any loss or damage which the NABARD may be put to, by reason of any act or default recoverable by the NABARD from the Vendor and to call upon the Vendor to maintain the deposit at the original limit by making further deposits.
- v. No interest will be allowed on performance bank guarantee.

## 20 Insurance

- i. The Bidder is responsible for acquiring insurance for all components, equipment and software. The goods supplied under the Contract shall be fully insured in Indian Rupees naming NABARD as the beneficiary.
- ii. The insurance shall be for an amount equal to 110% of the value of the goods from “warehouse to Final Destination” on “All Risks” basis including War Risks and Strike clauses valid for a period not less than 3 months after installation and commissioning and issue of acceptance certificate by NABARD.
- iii. Should any loss or damage occur, the Bidder shall :-
  - a. Initiate and pursue claim till settlement

- b. Promptly make arrangements for repair and/or replacement of any damaged item/s irrespective of settlement of claim by the underwriters.

## 21 Price Composition

- i. The price offered to NABARD must be in Indian Rupees only, inclusive of all applicable taxes and duties, packing forwarding, import and custom clearance, transportation, insurance till delivery at respective location, cost of installation commissioning and comprehensive on-site maintenance services under warranty etc..However, payment towards taxes would be made at actuals on production of original receipts only.
- ii. Duty /Entry tax, if applicable, will be reimbursed by NABARD at actual on production of original payment receipt.
- iii. From the date of placing the order till the delivery of the equipment, if any changes are brought in the tax structure by the Government resulting in reduction of the cost of the equipment , the benefits arising out of such reduction shall be passed on to NABARD.
- iv. Price quoted should be in multiple of ten only.
- v. The Vendors/Bidders should quote prices strictly as per the price composition stated above failing which the offers are likely to be rejected.

## 22 No Price Variations

The price shall be quoted by the Bidder in the specified Price-bid format given in **Annexure X** only. The price as finally agreed between the Vendor and NABARD shall be final and it shall not be subject to escalation for any reason whatsoever. In other words the commercial offer shall be on a fixed price basis. No upward revision in the prices would be considered on account of subsequent increases in government taxes, duties, levies, etc. However, if there is any reduction on account of government taxes, duties, local levies, etc. during the offer validity period, the same shall be passed on to NABARD.

## 23 Import Obligations

In the event of it being necessary to import any materials of foreign manufacture, the Vendor/Bidder should obtain the same against his own normal license quota and should not look to NABARD for any assistance whatsoever for their procurement.

## 24 Term of execution of work

The overall time limit for satisfactory Supply, Installation, Customization, Testing and Commissioning of NGFW solution shall be four (04) weeks from the date of acceptance of the work order. Time shall be the essence of the contract.

If the Vendor/Bidder fails to effect and complete the work within the time as stipulated as above, the Vendor/Bidder shall be liable to pay NABARD liquidated damages a sum of 1 % of the implementation cost for each completed day of delay in completion of work. The Vendors/Bidders aggregate liability to pay liquidated damages for the delay in completing the work shall not in any case exceed 25 % of the implementation cost.

## 25 Confidentiality

- i. The details of the proposed service shall be treated as confidential information between NABARD and Vendor/Bidder. Any such information shall not be passed on in part or in full to any third party without NABARD's prior written approval.
  - ii. Notice or other communications given or required to be given under the Contract shall be in writing and shall be hand-delivered with acknowledgment thereof, or transmitted by prepaid registered post or by recognized courier, or by facsimile, provided that where such notice is sent by facsimile, a confirmation copy shall be sent by pre-paid registered post or by recognized courier within five days of the transmission by facsimile, to the address of the receiving party by the other in writing, provided any change of address has been notified at least ten days prior to the date on which such notice has been given under the terms of the contract.
  - iii. Any notice or other communications shall be deemed to have validly given on date of delivery if hand-delivered; if sent by registered post or by recognized courier, then on the expiration of seven days from the date of posting; and if transmitted by facsimile, then on the next business date after the date of transmission.
  - iv. The Successful bidder shall not, without NABARD's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of NABARD in connection therewith, to any person other than a person employed by the Successful bidder in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
  - v. The Successful bidder shall not, without NABARD's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.
  - vi. The bidder either during the term or after the expiration of this contract shall not disclose any proprietary or confidential information relating to the project, the services, this contract, or NABARD's business or operations without the prior written consent of NABARD.
- N.B. Bidder is required to give undertaking in the format given in **Annexure XIII**.

## 26 Settlement of disputes by Arbitration:

- i. All disputes and differences of any kind whatsoever, arising out of or in connection with this Agreement or in the discharge of any obligation arising under this Agreement (Whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Agreement) shall be resolved amicably.
- ii. In case of failure to resolve the disputes and differences amicably within 30 days of the receipt of notice by the other party, then such unsettled dispute or difference shall be referred to arbitration by sole arbitrator mutually agreed in accordance with the Arbitration and Conciliation Act, 1996. If no agreement is arrived at within 30 days from the date of notice as

- to who shall be the sole arbitrator, then the sole arbitrator shall be appointed as hereinafter provided.
- iii. In case Vendor/Bidder raises a dispute and the same is referred to arbitration, NABARD shall send to Vendor/Bidder a list of three names of persons who shall be presently unconnected with NABARD or Vendor/Bidder. Vendor/Bidder shall on receipt of the names as aforesaid, select any one person so named to be appointed as sole arbitrator and communicate his name to NABARD within 30 days of receipt of the names. Vendor/Bidder shall thereupon without delay appoint the said person as the sole arbitrator. If Vendor/Bidder fails to select the person as sole arbitrator within 30 days of receipt of the panel NABARD shall be entitled to appoint one of the persons from the panel as sole arbitrator and communicate his name to Vendor/Bidder. If the person so appointed is unable or unwilling to act or refuses his appointment or vacates his office due to any reason whatsoever, another person shall be appointed by NABARD from the above list of persons.
  - iv. In case NABARD raises a dispute and the same is referred to arbitration, Vendor/Bidder shall send to NABARD a list of three names of persons who shall be presently unconnected with Vendor/Bidder or NABARD. NABARD shall on receipt of the names as aforesaid, select any one person out of the panel of three so named to be appointed as sole arbitrator and communicate his name to Vendor/Bidder within 30 days of receipt of the names. Vendor/Bidder shall thereupon without delay appoint the said person as the sole arbitrator. If NABARD fails to select the person as sole arbitrator within 30 days of receipt of the panel, Vendor/Bidder shall be entitled to appoint one of the persons from the panel as sole arbitrator and communicate his name to NABARD. If the person so appointed is unable or unwilling to act or refuses his appointment or vacates his office due to any reason whatsoever, another person shall be appointed by Vendor/Bidder from the above list of persons.
  - v. The Arbitration shall be governed by the Arbitration and Conciliation Act, 1996 as in force and as amended from time to time. The seat & venue of the same shall be in Mumbai. Where the parties appoint an Arbitrator, as per the procedure mentioned hereinabove, the award of the Arbitrator shall be final and binding on the parties. It is hereby agreed that in all disputes referred to the Arbitration, the Arbitrator shall give a separate award in respect of each dispute or difference in accordance with the terms of reference and the award shall be a reasoned award. It is hereby agreed that the Arbitrator shall not have powers to order any interim measures whatsoever during the course of arbitration.
  - vi. The fees, if any, of the Arbitrator shall initially be paid in equal proportion by each of the parties. The cost of the reference and of the award including the fees, if any, of the Arbitrator shall be directed to be finally borne and paid by such party or parties to the dispute in such manner or proportion as may be directed by the Arbitrator as the case may be in the award.
  - vii. All disputes arising out of or in any way connected with this Agreement shall be deemed to have arisen at Mumbai only and Courts in Mumbai only shall have jurisdiction to determine the same.
  - viii. The language of the proceedings shall be in English.

## 27 Order cancellation

NABARD reserves its right to cancel the entire/unexecuted part of the work contract at any time by assigning appropriate reasons in the event of one or more of the following conditions: -

- i. The selected bidder commits a breach of any of the Terms and conditions of the bid/ contract.
- ii. The bidder goes into liquidation voluntarily or otherwise is acquired / merged by another company within the contract duration.
- iii. Delay in delivery of the ordered equipment, etc. beyond three weeks from the date of acceptance of the work order (except with written permission from NABARD) or any instance where the progress regarding execution of contract, made by the selected bidder is found to be unsatisfactory.
- iv. Delay in installation and commissioning of the system beyond four weeks from the date of acceptance of the work order (except with written permission from NABARD).
- v. An attachment is levied or continues to be levied for a period of 7 days upon the effects of Bid.
- vi. Any other appropriate reason in view of NABARD.

In addition to the cancellation of the work contract, NABARD reserves the right to foreclose NABARD guarantee given by the Vendor/Bidder towards performance of the contract to appropriate the damages. NABARD further reserves the right to recover and adjust any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract or any other contract or order, against the cancellation if any of the Purchase/Work Order for any of the above mentioned reasons.

## 28 Right to Accept or Reject the Quotation

NABARD does not bind itself to accept the lowest bid or any or all Quotations and reserves to itself the right to accept or reject any or all the 'Quotations', either in whole or in part without assigning any reasons for doing so. If any conditions are stipulated, at the time of submission of 'Quotations', they will be liable to be summarily rejected.

## 29 Right to alter quantities/components

NABARD reserves the right to alter quantities and/or components of NGFW solution to be purchased on the same terms and conditions under CVC guidelines. NABARD may place this order once again as repeat order in future in full or in part thereof (within the price validity period as per Section No. 5(ii)) to the successful bidder based on their requirement in future if any. NABARD reserves the rights to alter quantities, revise/modify all or any of the specifications, delete some items specified in this offer, when finalizing its requirements or declare the RFP void before or after receiving the responses. NABARD also reserves the right to buy any or all of the products meeting the stated requirement. The Bank also reserves the right to procure Hardware separately from a different vendor. NABARD will have the option to split the orders for different products among the quoting vendors.

## 30 Force Majeure

In case either party is prevented from performing any of its obligations due to any cause beyond its control, including but not limited to act of God, fire, flood, explosion, war, action or request of governmental authority, systemic breakdown, failure of electricity supply, accident and labor trouble, the time for performance shall be extended until the operation or such cause has ceased, provided the party affected gives prompt

notice to the other party of any such factors or inability to perform and resume performance as soon as such factors disappear or are circumvented. Decision of NABARD in this regard shall be final and shall not be questioned in arbitration or other legal proceedings.

## 31 Evaluation Process

The evaluation process will include:

- i. Technical evaluation of RFP response, which include scrutiny of proposal to ensure that the Vendor/Bidder meets the eligibility criteria, has implementation experience, equipment offered comply with functional & technical specifications etc.
- ii. The Commercial Bid of the technically qualified Vendors/Bidders will be opened on the date and time to be notified later.
- iii. The work order will be issued to the L1 vendor. The successful bidder shall acknowledge the receipt of the work order within 02 days from the date of work order and shall there by confirm their acceptance of the work order in its entirety without exceptions by returning duplicate copy of work order duly signed and stamped in token of their acceptance. The bidder should start working on the project within 05 days of the acceptance of the work order failing which NABARD reserve the right to forfeit EMD amount from the successful bidder (refer Section No. 11.1).
- iv. The final decision regarding selection of Vendor/Bidder will be taken by NABARD.
- v. The implementation of the project will commence upon successful negotiation of a contract between NABARD and the selected Vendor/Bidder. NABARD reserves the right to reject any or all proposals fully or partially. Similarly, NABARD reserves the right to include or not to include any Vendor/Bidder in the final short-list.

### 31.1 Technical Evaluation

Table:1 The technical evaluation will be done based on the parameter and weightage mentioned below:-

| S.N          | Evaluation Criteria   | Weightage  |
|--------------|---|------------|
| 1            | Implementation Experience (Successfully completed)  | 10         |
| 2            | Technical Capability (H/w & S/w features, Bidder's Capability, Maintenance & Support)       | 30         |
| 3            | Financial Capability  | 10         |
| 4            | Next Generation Firewall - Actual Technical Score   | 20         |
| 5            | TAMD document   | 10         |
| 6            | Visit to the sites where vendor has implemented such solutions / Discussion with the client | 10         |
| 7            | Technical Presentation  | 10         |
| <b>Total</b> |   | <b>100</b> |

### 31.2 Commercial:

The details of commercial format has been given in Annexure X



Table 2: Weighted Total Price:-

| Sl.No        | Cost Components                   | Weightage  |
|--------------|-----------------------------------|------------|
| 1            | Firewall Cost                     | 50         |
| 2            | Implementation                    | 10         |
| 3            | AMC, Warranty & Support (5 Years) | 25         |
| 4            | On-Site Support                   | 10         |
| 5            | Training                          | 05         |
| <b>Total</b> |                                   | <b>100</b> |

N.B. Prices will be multiplied by the multiplying factor and then the sum of the individual components will be divided by 100 to arrive at the Weighted Total Price. This Weighted Total Price will be considered for 30% of the commercials

### 31.3 Formula for final evaluation

#### Technical Assessment (70% weightage)

- i. Full marks i.e. 100 (absolute value) will be awarded to the bidder scoring the highest marks based on parameters & their corresponding weightage given in Table 1.
- ii. Proportionate marks will be awarded to other bidders as a percentage of the highest marks.
- iii. Full 70 marks will be awarded to the bidder getting the highest marks.
- iv. Similarly proportionate marks will be awarded to the other bidders.

#### Commercial Assessment (30% weightage)

- i. Full marks i.e. 100 (absolute value) will be awarded to the bidder quoting the lowest price i.e. Total Contract Value as per Weighted Total Price.
- ii. Proportionate marks will be awarded to the other bidders as a percentage of the lowest quote.
- iii. Full 30 marks will be awarded to the bidder quoting the lowest price i.e. 30% of 100 i.e. 30. Similarly proportionate marks will be awarded to absolute value quoted by other bidders.

#### Overall Assessment for calculation of L1:

- i. Marks scored in Technical Assessment and Commercial Assessment will be added.
- ii. The bidder scoring the highest marks will be L1.
- iii. Evaluation process as decided by NABARD will be binding to the bidders.
- iv. NABARD in its sole/absolute discretion can apply whatever criteria deemed appropriate in determining the responsiveness of the proposal submitted by the respondents. NABARD may reject any / all proposal(s) at any stage without assigning any reason thereof.

N.B. For detailed calculation refer **Schedule 4** of the RFP



Annexure I (RFP Download Declaration)

To,  
The Chief General Manager  
Department of Information Technology,  
National Bank for Agriculture and Rural Development  
Fifth floor, C Wing,C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.

Sir,  
Sub: .....

Kindly refer to your RFP No. .... published on the website ..... downloaded from electronic media. We wish to confirm that we have downloaded the complete RFP document from the website /electronic media. We shall submit the RFP document as per your prescribed specifications for Technical & Commercial Bid.

I/We have downloaded this RFP document from the internet site ..... electronic media and I/we have not tampered / modified the RFP forms in any manner. In case, if the same is found to be tampered / modified, I / we understand that my / our bid will be summarily rejected and full earnest money deposit, if any will be forfeited and I/we am/are liable to be banned from doing business with NABARD / other PSUs and/or prosecuted.

I /We shall submit a signed copy of the RFP, as a token of acceptance of all the terms & conditions mentioned in the RFP.

**Date: Signature of Tenderer with Seal:**

**Phone:**

**Fax No. :**

**E-mail address:**



Annexure II (Letter of Authorization)

To,  
**The Chief General Manager**  
**Department of Information Technology,**  
**National Bank for Agriculture and Rural Development**  
**Fifth floor, C Wing, C-24, 'G' Block, Bandra-kurla Complex,**  
**P.B. No. 8121, Bandra (East),**  
**Mumbai - 400 051.**

Dear Sir,

We \_\_\_\_\_(name of the company) have submitted our bid for participating in Bank's RFP dated \_\_\_\_\_ for \_\_\_\_\_. We also confirm having read and understood the terms of RFP as well as the scope of work & requirements.

As per the terms of RFP , we nominate Mr. \_\_\_\_\_, designated as \_\_\_\_\_ of our company to participate in the bidding process. NABARD shall contact the above named official for any and all matters relating to the bidding process.

We, hereby confirm that we will honor the Bids placed by Mr. \_\_\_\_\_ on behalf of the company in the bidding process, failing which we will forfeit the EMD. We agree and understand that the NABARD may debar us from participating in future tenders for any such failure on our part.

***Signature with company seal***

***Name –***

***Company / Organization –***

***Designation within Company / Organization –***

***Address of Company / Organization –***

***Name of Authorised Representative***

***Designation of Authorised Representative***

***Signature of Authorised Representative***

***Verified by***

***Signature of Verifying Authority & Date***



## Annexure III (Organizational Profile)

### Organisational / Financial PROFILE OF THE VENDOR/BIDDER

|  |   |                                  |           |   |
|--|---|----------------------------------|-----------|---|
| Constitution   | Proprietary/Partnership/Private Ltd./Public Ltd. <i>(Tick one)</i>  |                                  |           |   |
| Established since (MM/YY)  |   |                                  |           |   |
| Address of Registered Office   |   |                                  |           |   |
| Classification   | <ul style="list-style-type: none"> <li>• Service Provider/System Integrator</li> <li>• Consultancy Firm</li> <li>• IT security Firm</li> <li>• Hardware Vendor/OEM</li> <li>• Software Developer</li> <li>• Service Support Co.</li> <li>• Others (please specify)</li> </ul> |                                  |           |   |
| If Joint Venture, then specify names of Partners in the JV   |   |                                  |           |   |
|  | <b>Name</b>   | <b>Position/Designation</b>      |           |   |
| Name(s) of Proprietor(s) / Partner(s) / Directors  | 1   |                                  |           |   |
|  | 2   |                                  |           |   |
| Details of resources having skills to support and execute the said activity  | Name  | Certifications / Relevant Degree | Total No. | Name & Experience of the most experienced resource in this category |
|  | 1   |                                  |           |   |
|  | 2   |                                  |           |   |
|  | ..  | etc                              |           |   |
| Total Number of Employees  |   |                                  |           |   |
| Number of locations where Service Support Centers are available for catering to the Product /Services being supplied |   |                                  |           |   |
|  | 1   |                                  |           |   |



|  |   |  |                                   |   |
|--|---|--|-----------------------------------|---|
| List of products deployed/serviced offered   | 2   |  |                                   |   |
| Major Service/product  |   |  |                                   |   |
| Business Figures for 3 years<br>copies of supporting documents to be enclosed  | Turnover (Rs. Lakh)   | Net Profit (Rs. Lakh)                      |                                   |   |
|  | Financial Year 2016-17  |  |                                   |   |
|  | Financial Year 2015-16  |  |                                   |   |
|  | Financial Year 2014-15  |  |                                   |   |
| List of reputed major Corporate Customers to whom the similar solution/services have been provided for a period of in last 5 years | <p><i>Please furnish details in the following format.</i></p> <p><i>N.B : Bidder is required to assist NABARD in case of reference is required.</i></p> |  |                                   |   |
| Name and address of the Organization with phone number   | Duration (From date – To date)  | Brief details of services/products offered | Approx. Value of Order (Rs. Lakh) | Contact Person with the contact details |
|  |   |  |                                   |   |
|  |   |  |                                   |   |
|  |   |  |                                   |   |

**Signature of Vendor/Bidder :** \_\_\_\_\_

**Name:** \_\_\_\_\_



Annexure IV (Project List)

List of similar projects executed by the vendor in last 5 years:-

| S/N | Activity | Brief description of work | Indian customers |     |      |        | Abroad | Total | Remarks, if any |
|-----|----------|---------------------------|------------------|-----|------|--------|--------|-------|-----------------|
|     |          |                           | BFSI             | PSU | Govt | Others |        |       |                 |
| 1.  |          |                           |                  |     |      |        |        |       |                 |
| 2.  |          |                           |                  |     |      |        |        |       |                 |
| 3.  |          |                           |                  |     |      |        |        |       |                 |
| 4.  |          |                           |                  |     |      |        |        |       |                 |
| 5.  |          |                           |                  |     |      |        |        |       |                 |
| 6.  |          |                           |                  |     |      |        |        |       |                 |
| 7.  |          |                           |                  |     |      |        |        |       |                 |
| 8.  |          |                           |                  |     |      |        |        |       |                 |
| 9.  |          |                           |                  |     |      |        |        |       |                 |
| 10. |          |                           |                  |     |      |        |        |       |                 |
| ... |          |                           |                  |     |      |        |        |       |                 |

N.B: An activity performed more than once in the same organization / sector will be counted as many times as it was performed there.

## Annexure V (Black List)

### **Declaration that the Bidder is not any other BANK/ PSU's / Govt.'s Vendor BLACK-LIST**

#### **Part A) In the case of a Proprietary Concern:**

I hereby declare that neither I in my personal name or in the name of my Proprietary concern M/s. \_\_\_\_\_ which is submitting the accompanying Bid/Tender nor any other concern in which I am proprietor nor any partnership firm in which I am involved as a Managing Partner have been placed on black list declared by any Bank , Financial Institution , Govt's Vendor Black List except as indicated below:

(Here give particulars of blacklisting and in absence thereof state "NIL")

#### **Part B) In the case of a Partnership Firm :**

We hereby declare that neither we, M/s. \_\_\_\_\_, submitting the accompanying Bid/Tender nor any partner involved in the management of the said firm either in his individual capacity or as proprietor or managing partner of any firm or concern have or has been placed on blacklist declared by any Bank , Financial Institution , Govt's Vendor Black List, except as indicated below

(Here give particulars of blacklisting and in the absence thereof state "NIL")

#### **Part C) In the case of Company:**

We hereby declare that we have not been placed on any black list declared by any Bank , Financial Institution , Govt's Vendor Black List , except as indicated below:

(Here give particulars of black listing and in the absence thereof state "NIL")

It is also understood that if this declaration is found to be false in any particular, NABARD shall have the right to reject my/our bid, and if the bid has resulted in a contract, the contract is liable to be terminated.

**Place: Signature of Bidder:** \_\_\_\_\_

**Date: Name of Signatory:** \_\_\_\_\_

## Annexure – VI Forwarding Letter (Technical Bid)

**To,  
The Chief General Manager  
Department of Information Technology,  
National Bank for Agriculture and Rural Development  
Fifth floor, C Wing, C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir,

With reference to Request for Proposal (RFP) Ref No. RFP No: \_\_\_\_\_ dated \_\_\_\_\_, including all annexures & schedules, the receipt of which is hereby duly acknowledged, I/we, the undersigned offer to provide the desired solution and services for the NABARD's IT assets at select business units of the NABARD in conformity with the terms and conditions of the said RFP and in accordance with our proposal and the schedule of Prices indicated in the Price Bid and made part of this bid. If our Bid is accepted:-

1. I/We undertake to complete the project within the scheduled time lines.
  3. I/We confirm that this offer is valid for six months from the last date for submission of RFP to the Bank.
  4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
  5. I/We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
  6. I/We agree that the Bank is not bound to accept the lowest or any Bid that the Bank may receive.
  7. I/We have not been barred/black-listed by any regulatory / statutory authority in India and we have required approval, if any, to be appointed as a service provider.
  8. I/We shall observe confidentiality of all the information passed on to us in course of the tendering process and shall not use the information for any other purpose than the current tender.
  9. I/We confirm that we have obtained all necessary statutory and obligatory permission to carry out the assignment, if any.
  1. I/We undertake to deliver the goods/ provide the services in accordance with the Delivery Schedule / implementation schedule specified.
  2. I/We further undertake that we fulfill the minimum eligibility criteria mentioned in RFP.
- If our bid is accepted, we will obtain the guarantee of a Bank in a sum equivalent to 10% per cent of the Contract Price for the due Performance of the Contract, in the form prescribed by NABARD.
3. We agree to abide by this bid during validity of the bid and may be accepted at any time before the expiration of that period.

WE FURTHER CONFIRM THAT,

1. Our offer is valid for a period of 60 days from the last date (revised last date if such date is extended by NABARD) for submission of the bid .





2. In case we offer system and/or other software manufactured by another company, such software operates effectively on the system offered by us and we are willing to accept responsibility for its successful operations.
3. Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your Notification of Award, shall constitute a binding Contract between us.
4. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
5. I/We understand that you are not bound to accept the lowest or any bid you may receive.

***(Signature)***

***(name & designation)***

***(Name & Address of the Bidder with Seal)***



## Annexure VII (Technical Parameters)

Marks (Yes :1 No:0 for each of the two columns)

| S/N                        | Features   | Features Present or Not (Either Yes or No) | If present whether offered or not (Yes or No) | Marks | Remarks, if any |
|----------------------------|--|--|---|-------|-----------------|
| <b>General Requirement</b> |  |  |   |       |                 |
| 1.                         | The proposed solution should be latest model of Next Generation firewall stable for more than 01 year  |  |   |       |                 |
| 2.                         | The proposed security solution should either be in the Leader’s quadrant or Challenger’s quadrant in the latest Gartner "Magic Quadrant for Enterprise Network Firewalls"  |  |   |       |                 |
| 3.                         | For the solution proposed security check updates do not require reboot.  |  |   |       |                 |
| 4.                         | The Firewall system should have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution  |  |   |       |                 |
| 5.                         | The NGFW should have integrated IPS, Antimalware Anti BoT, Antivirus, IPSec VPN, Bandwidth Management, DPI, Application Control and user control & awareness.  |  |   |       |                 |
| 6.                         | The Firewall architecture should be on distributed framework i.e, NGFW with Threat Prevention Policy Management, Logging, Reporting Dashboard etc.   |  |   |       |                 |
| 7.                         | Proposed solution should have provision of immutable audit trail wrt all changes done on policy management dashboard.  |  |   |       |                 |
| 8.                         | The communication between all the components should be encrypted with SSL or PKI.  |  |   |       |                 |
| 9.                         | Licensing model should be device based and not on user or any other parameter based  |  |   |       |                 |
| 10.                        | Every Gateway Security control( like Firewall or any other feature required to meet the Specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise. |  |   |       |                 |
| 11.                        | The solution should support load balancing of multiple Internet links terminated on it.  |  |   |       |                 |
| 12.                        | The proposed solution should have an Multi-tier engine to detect & Prevent Command and Control IP/URL and DNS  |  |   |       |                 |

|     |  |  |  |  |  |
|-----|--|--|--|--|--|
| 13. | The solution should be appliance based and have hardened OS for Gateway appliance.   |  |  |  |  |
| 14. | Appliance should support for Active – Active connections. It should not depend upon any 3rd party product or alliance for the same.  |  |  |  |  |
| 15. | The system should not have any back door vulnerability in their product or OS for last two year ending on or after last date of submission or extended last date of submission of RFP.   |  |  |  |  |
| 16. | Proposed Solution framework should have IPSec VPN (Site to Site VPN) and SSL VPN functionalities for Secure Remote access to corporate application over the internet via endpoint i.e, Smartphones or PC's, Tablets and Laptops  |  |  |  |  |
| 17. | The solution should support static, dynamic routing protocols like RIPv2, BGPv4, OSPF etc.   |  |  |  |  |
| 18. | The proposed Hardware should not have End of Sale for next 03 (Three) years  |  |  |  |  |
| 19. | The proposed Hardware should not have End of Sale for next 06 (Six) years  |  |  |  |  |
| 20. | Solution should have hardened OS & latest firmware for all appliances.   |  |  |  |  |
| 21. | Appliance should support plug & play Active – Active connections without any dependency on any other tool.   |  |  |  |  |
| 22. | The appliance hardware should be a multicore CPU architecture.   |  |  |  |  |
| 23. | The vendor should ensure that there is SPOC from OEM throughout the project period and OEM must provide 24 X 7 X 365 technical support. The OEM must provide the dedicated login credentials to NABARD with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. NABARD should be able to raise tickets directly to OEMs. |  |  |  |  |
| 24. | The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM   |  |  |  |  |
| 25. | Any third party product required to achieve the func-  |  |  |  |  |

|                              |   |  |  |  |  |
|------------------------------|---|--|--|--|--|
|                              | tionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc.          |  |  |  |  |
| 26                           | Performance tuning such that the solution operates as proposed on the production network  |  |  |  |  |
| 27                           | The Firewall must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth of approx. 10% per annum |  |  |  |  |
| 28                           | The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 10 Virtual Firewall license.   |  |  |  |  |
| 29                           | The proposed system should have integrated Traffic Shaping functionality.   |  |  |  |  |
| 30                           | The Firewall should belong to a family of products that is NSS/NIST Approved and IPv6 ready   |  |  |  |  |
| 31                           | The proposed product should have the ability to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM and using any application.  |  |  |  |  |
| 32                           | Should have built in pattern database and option to configure new patterns as and when required and should have full archive features for http, https, ftp, ftps & email protocols      |  |  |  |  |
| 33                           | The solution should create configuration templates to quickly provision devices for mass deployment   |  |  |  |  |
| 34                           | The proposed solution must offer centralized management appliance to manage all firewall devices from data centre.  |  |  |  |  |
| 35                           | The vendor should provide admin level training to NABARD's identified personnel in authorized training center and by qualified and certified instructor.                                |  |  |  |  |
| <b>Architecture Features</b> |   |  |  |  |  |
| 1                            | Firewall Appliances should be deployed for Active – Active or Active -Passive failover architecture for both Firewall & VPN functions as and when required.                             |  |  |  |  |
| 2                            | The solution should support dual Stack with IPv4 and IPv6 functionality ready.  |  |  |  |  |

|   |   |  |  |  |  |
|---|---|--|--|--|--|
| 3   | Product should support the IPSec VPN for both Site - Site & Remote access VPN   |  |  |  |  |
| 4   | Firewall system should support virtual tunnel interfaces to provision Route -Based IPSec VPN  |  |  |  |  |
| 5   | The firewall should support ISP link load balancing.  |  |  |  |  |
| 6   | The firewall must support stateful active active load balancing and high availability for redundancy.   |  |  |  |  |
| 7   | Firewall should support Link Aggregation functionality to group multiple ports as single port.  |  |  |  |  |
| 8   | Firewall should support Ethernet Bonding functionality for Full Mesh deployment architecture  |  |  |  |  |
| 9   | The Firewall should support a minimum of 8 x GE RJ45, 8x GE SFP , 8x10G SFP+ (4 Populated with SR) & 1xGE Management & 1 Console interfaces with auto sensing capacity and option to expand further.                            |  |  |  |  |
| 10  | Should support automatic ISP failover as well as ISP load sharing   |  |  |  |  |
| <b>Network Protocol/Standards supported</b> |   |  |  |  |  |
| 1   | The product's Firewall Modules should support the deployment in Routed as well as Transparent Mode and support web proxy/SSL proxy  |  |  |  |  |
| 2   | All internet based applications should be supported for filtering like Telnet, FTP, SMTP, HTTP, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, Ms -Exchange etc.   |  |  |  |  |
| 3   | Solution should support option to integrate with Email/SMS/token based 2FA for Internal as well as VPN users authentication.  |  |  |  |  |
| 4   | IPSec VPN should support the Authentication Header Protocols – MD5 & SHA .  |  |  |  |  |
| 5   | IPSec ISAKMP methods should support Diffie -Hellman Group 1,2,5,14 & 19, MD5 & SHA Hash, RSA & Manual Key Exchange & Authentication, 3DES/AES -256 Encryption of the Key Exchange Material and algorithms like RSA -1024 / 1536 |  |  |  |  |
| 6   | IPSec encryption should be supported with 3DES, AES -128 & AES -256 standards .   |  |  |  |  |
| 7   | It should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, DVMRP protocols.  |  |  |  |  |

|                                 |   |  |  |  |  |
|---------------------------------|---|--|--|--|--|
| 8                               | IPSec encryption should be supported with 3DES, AES - 128 & AES -256 standards .  |  |  |  |  |
| 9                               | Firewall should support PKI Authentication with PCKS#7 & PCKS#10 standards.   |  |  |  |  |
| 10                              | It should support at least 200 protocols.   |  |  |  |  |
| 11                              | The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs  |  |  |  |  |
| 12                              | The Firewall should support Inbound Port Forwarding with inbound Load Balancing if servers are running in high availability (layer 4)   |  |  |  |  |
| 13                              | The Firewall should support deployment of Virtualization at least for 5 virtual context from the day one without any additional cost / licenses & must be upgradable upto 100 by addition license                                       |  |  |  |  |
| 14                              | Virtual context must have all security features for use for every single firewall   |  |  |  |  |
| 15                              | The proposed system shall support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional cost for license or solution for VPN client and also IPSEC (DES, 3DES, AES) encryption/decryption and SSL encryption/decryption |  |  |  |  |
| <b>Performance Requirements</b> |   |  |  |  |  |
| 1                               | The solution should not have latency more than 10 microseconds  |  |  |  |  |
| 2                               | The proposed solution should deliver more than 5 Gbps NGTP throughput enabling Firewall, IPS, Application Control, URL filter, Antivirus, AntiBot etc.  |  |  |  |  |
| 3                               | Firewall Throughput should be min 20 Gbps   |  |  |  |  |
| 4                               | IPS Throughput should be min 4 Gbps with all IPS features enabled.  |  |  |  |  |
| 5                               | The product should have TLS/SSL throughput min 2 Gbps   |  |  |  |  |
| 6                               | Full DPI throughput should be min 4 Gbps  |  |  |  |  |
| 7                               | IPSec VPN throughput should be min 5 Gbps   |  |  |  |  |

|                     |   |  |  |  |  |
|---------------------|---|--|--|--|--|
| 8                   | SSL VPN Throughput should be min 2 Gbps   |  |  |  |  |
| 9                   | Application Control Throughput should be min 4 Gbps   |  |  |  |  |
| 10                  | AntiMalware throughput should be min 2 Gbps   |  |  |  |  |
| 11                  | It should support minimum 1 million concurrent connections  |  |  |  |  |
| 12                  | It should support min 50,000 connections per second   |  |  |  |  |
| 13                  | It should support min 10,000 users  |  |  |  |  |
| 14                  | It should support minimum 10,000 policies   |  |  |  |  |
| 15                  | Appliance should be supplied with at least 16GB RAM upgradable upto 32 GB using additional memory in the same slot. However, higher configuration would be preferred. |  |  |  |  |
| 16                  | Solution should support Link Aggregation to achieve higher bandwidth  |  |  |  |  |
| 17                  | The Firewall must provide NAT functionality, including dynamic and static NAT translations.   |  |  |  |  |
| 18                  | Solution should support IPv6 NAT functionality NAT64 and NAT46  |  |  |  |  |
| 19                  | Solution should be supplied with High Availability with Active-Active LS functionality  |  |  |  |  |
| 20                  | The proposed solution should have an integrated solution for IPSEC, site to site, Client to site, and SSL VPN.  |  |  |  |  |
| 21                  | Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy roll-backs during the version upgrades                            |  |  |  |  |
| 22                  | HA solution deployed should support smooth upgrade for both Major and Minor codes   |  |  |  |  |
| 23                  | The solution should support 40G QSFP+ for future expansion.   |  |  |  |  |
| 24                  | Firewall should have Redundant dual hotswappable power supplies, redundant hard disks and cooling fans.   |  |  |  |  |
| 25                  | Appliance should have a capability to support for more than 256 VLANs   |  |  |  |  |
| <b>IPS Features</b> |   |  |  |  |  |
| 1                   | IPS Engine should support Vulnerability and Exploit sig-  |  |  |  |  |

|    |   |  |  |  |  |
|----|---|--|--|--|--|
|    | natures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation.   |  |  |  |  |
| 2  | The IPS should be constantly updated with new defenses against emerging threats   |  |  |  |  |
| 3  | IPS should activate protection for both Client Protection and Server Protections  |  |  |  |  |
| 4  | IPS should provide protection for OWASP top 10 Website Vulnerability Classes  |  |  |  |  |
| 5  | IPS updates should have both options of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time  |  |  |  |  |
| 6  | IPS should have advanced capabilities that detect and prevent attacks launched against the Web infrastructure   |  |  |  |  |
| 7  | IPS should have the functionality of Geo Protection to Block the traffic country wise.  |  |  |  |  |
| 8  | IPS should provide Protection against Injection Vulnerabilities SQL Injection, Command Injection, LDAP Injection, HTTP Command Injection  |  |  |  |  |
| 9  | Blocking SQL and Commnad Injection by Keywords traced in form field GET, POST etc   |  |  |  |  |
| 10 | Should have a provision to configure blocking of Distinct and Non-Distinct SQL Commnads, Shell Commands etc.  |  |  |  |  |
| 11 | IPS should provide Appliction layer protections for Cross site scripting, Directory traversal etc   |  |  |  |  |
| 12 | Specific vulnerabilities keywords that can be used for scripting code, JavaScript and VBScript. commands, event that can trigger scripting engine, and HTML attributes and tags.              |  |  |  |  |
| 13 | Protection against Malicious code for Buffer Overflow, Heap overflow and other malicious executable code attacks that target Web servers and other applications without the need of signature |  |  |  |  |
| 14 | Monitor web communication for potential executable code, confirms the presence of executable code and identifies whether the executable code is malicious                                     |  |  |  |  |
| 15 | Protections against Information disclosure for Header   |  |  |  |  |



|    |   |  |  |  |  |
|----|---|--|--|--|--|
|    | spoofing enforcement, directory listing prevention, error concealment , HTTP Protocol Inspections for HTTP format size enforcement, ASCII-only request enforcement, ASCII-only response header enforcement, header rejection definitions, HTTP method definitions |  |  |  |  |
| 16 | Protection for HTTP Clients using IE for COM (Component Object Model) and DOM (Document Object Model).  |  |  |  |  |
| 17 | Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.   |  |  |  |  |
| 18 | Should have Sandbox for new protections.  |  |  |  |  |
| 19 | IPS Profile should have an option to select or re-select specific signatures that can be activated/de-activated as per Bank's environment   |  |  |  |  |
| 20 | IPS should also have IPS should have an option to create your own signatures with an open signature language.   |  |  |  |  |
| 21 | Configuration granularity for Individual servers protected by Web Intelligence attack protections enabled for each sever; for each attack protection, apply to individual servers or inspect all HTTP traffic; customisable profiles associated.                  |  |  |  |  |
| 22 | Solution should have software bypass IPS function based on configured threshold of CPU, Memory.   |  |  |  |  |
| 23 | Real time safeguard and defense updates through update service  |  |  |  |  |
| 24 | IPS should understand Denial of Service tool used to crafts and send multiple HTTP Request that can potentially cause attcahed system to become temporarily unresponsive  |  |  |  |  |
| 25 | It should be able to take below actions<br>a. Add IP to Quarantine List<br>b. Restrict no of HTTP Request from same source and destination<br>c. Time in which HTTP Request arrive and source IP will be blocked<br>d. Packet Capture                             |  |  |  |  |
| 26 | Should have an understanding of DDOS Tool Kit including SYN Flood, UDP Flood, DNS Query flood and GET floods  |  |  |  |  |

|    |  |  |  |  |  |
|----|--|--|--|--|--|
| 27 | Should have protection against exploitation of DOS vulnerability in Microsoft IE, Microsoft IIS, Apache, Oracle etc.   |  |  |  |  |
| 28 | Prevent and Block attempts to exploit DOS related vulnerability in applications  |  |  |  |  |
| 29 | Integrated IPS functionality should be available as a software module that can be activated and de-activated as and when required.   |  |  |  |  |
| 30 | IPS should have advanced capabilities that detect and prevent attacks launched against the Web infrastructure  |  |  |  |  |
| 31 | Activation of new protections based on parameters like Performance impact, Confidence index, Threat severity etc.  |  |  |  |  |
| 32 | File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance   |  |  |  |  |
| 33 | IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, Industry Reference etc.           |  |  |  |  |
| 34 | IPS events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis |  |  |  |  |
| 35 | Intrusion Prevention should have an option to add exceptions for network and services.   |  |  |  |  |
| 36 | IPS Policy to Block the traffic by country should have an option to configure in incoming direction, Outgoing direction or both.   |  |  |  |  |
| 37 | Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.  |  |  |  |  |
| 38 | Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance.   |  |  |  |  |
| 39 | Should have prevention against Script DDoS tool that utilizes high bandwidth web servers to generate malicious DDoS traffic.   |  |  |  |  |
| 40 | Firewall must be able to scan http, https, IMAP, IMAPs, FTP, FTPs, POP, POPs, SMTP, SMTPs & MAPI protocols with AV signatures  |  |  |  |  |
| 41 | File reassembly and data filtering for more than 20 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 100 file type                            |  |  |  |  |

|    |  |  |  |  |  |
|----|--|--|--|--|--|
| 42 | Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks  |  |  |  |  |
| 43 | Cloud-based URL filtering with a URL category database that contains over 130 million URLs in over 80 categories   |  |  |  |  |
| 44 | Defense against web application attacks, such as cross-site scripting and SQL injection attacks  |  |  |  |  |
| 45 | Supports APT defense. Interworking with the Sandbox to detect and block the malicious files in the network.  |  |  |  |  |
| 46 | IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available               |  |  |  |  |
| 47 | IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups. |  |  |  |  |
| 48 | Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)   |  |  |  |  |
| 49 | In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and Firewall should continue to operate while the IPS problem is being resolved   |  |  |  |  |
| 50 | Supports attack recognition inside IPv6 encapsulated packets   |  |  |  |  |

**Anti Malware & Anti-Bot**

|   |  |  |  |  |  |
|---|--|--|--|--|--|
| 1 | The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family                   |  |  |  |  |
| 2 | The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots |  |  |  |  |
| 3 | The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS   |  |  |  |  |

|    |  |  |  |  |  |
|----|--|--|--|--|--|
| 4  | The Proposed solution should not allow patient zero in network. It should block malware entry in real-time.  |  |  |  |  |
| 5  | The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations                   |  |  |  |  |
| 6  | The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities                                  |  |  |  |  |
| 7  | The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware                |  |  |  |  |
| 8  | The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.             |  |  |  |  |
| 9  | Proposed solution should have feature to hold connection or file unless classification completes. Vendor should provide relevant document to support claim.                        |  |  |  |  |
| 10 | Solution should be able to discover the Bot infected machine   |  |  |  |  |
| 11 | Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc   |  |  |  |  |
| 12 | Anti-virus scanning should support proactive and stream mode   |  |  |  |  |
| 13 | Solution should be able to create a protection scope for the inspection  |  |  |  |  |
| 14 | Proposed solution should have an option of configuring Exception   |  |  |  |  |
| 15 | Anti-spyware for pattern based blocking at the gateway   |  |  |  |  |
| 16 | The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)  |  |  |  |  |
| 17 | The proposed solution should be able to detect & prevent the malware by scanning different file types.   |  |  |  |  |
| 18 | The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, FTPS, POP3, POP3S IMAP, IMAPS, SMTP &SMTPS. |  |  |  |  |

|    |   |  |  |  |  |
|----|---|--|--|--|--|
| 19 | The proposed solution should prevent the users to access the malware hosting websites and/or web resources  |  |  |  |  |
| 20 | The Anti-Virus should Scan files that are passing on CIFS protocol  |  |  |  |  |
| 21 | The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information eXpression)  |  |  |  |  |
| 22 | The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution configured over common threat intelligence exchange methodology, called as TAXII (Trusted Automated eXchange of Indicator Information) |  |  |  |  |
| 23 | The proposed solution should support archive scanning & should be able to support deep inspection scanning.   |  |  |  |  |
| 24 | Solution should support fail-open or fail-close in case of system error   |  |  |  |  |
| 25 | Solution should be able to create a protection scope for the inspection   |  |  |  |  |
| 26 | Solution should be able to create a protection scope for the inspection   |  |  |  |  |
| 27 | Proposed solution should have an option of configuring Exception to exclude scanning  |  |  |  |  |
| 28 | The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)   |  |  |  |  |
| 29 | Solution should give information related to Performance impact and confidence level of protections while creating profiles.   |  |  |  |  |
| 30 | Solution should be able to identify malwares coming from incoming files and malwares downloaded from Internet.  |  |  |  |  |

|                                    |   |  |  |  |  |
|------------------------------------|---|--|--|--|--|
| 31                                 | Firewall must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.                            |  |  |  |  |
| 32                                 | Firewall should offer both anti-virus scanning options - proxy mode and flow (streaming) mode.  |  |  |  |  |
| 33                                 | Solution must provide option to create custom signature for applications  |  |  |  |  |
| 34                                 | Atleast 2000+ application signature must be there & it should able to understand well known application like P2P, Voice, etc without any dependency on the port   |  |  |  |  |
| 35                                 | Provides over 5000 signatures for attack identification.  |  |  |  |  |
| <b>Identity Awareness Features</b> |   |  |  |  |  |
| 1                                  | Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement  |  |  |  |  |
| 2                                  | Firewall should support the Identity based logging, application detection and usage controls  |  |  |  |  |
| 3                                  | Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc   |  |  |  |  |
| 4                                  | Should have Categories like Business Applications, IM, File Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Sarch Engine, Virtual Worlds, Webmail etc                               |  |  |  |  |
| 5                                  | The proposed solution must delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.). |  |  |  |  |
| 6                                  | Identity Access should be able to distinguish between employee and other like guests and contractors.   |  |  |  |  |
| 7                                  | Should have an option of time duration for Guests Login.  |  |  |  |  |
| 8                                  | Should provide seamless AD Integration with multiple deployment options like Clientless, Captive Portal or Identity Agent.  |  |  |  |  |

|                            |   |  |  |  |  |
|----------------------------|---|--|--|--|--|
| 9                          | Active Directory user's identification may be done either through querying Active Directory, through a captive portal or through installing a one-time, thin client-side agent                              |  |  |  |  |
| 10                         | Identity awareness licensing should be passed per gateway and not restrict on the basis on users.   |  |  |  |  |
| 11                         | Should support redundancy High Availability and Load Sharing.   |  |  |  |  |
| 12                         | Identity Awareness should work in conjunction with Application Control.   |  |  |  |  |
| 13                         | Should support and obtain the user identity in case user is behind a proxy.   |  |  |  |  |
| 14                         | The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.   |  |  |  |  |
| 15                         | Atleast 2500+ application signature must be there & it should able to understand welknown application like P2P, Voice, etc without any dependency on the ports  |  |  |  |  |
| <b>Application Control</b> |   |  |  |  |  |
| 1                          | Application control database must contain more than 6000 known applications   |  |  |  |  |
| 2                          | Should have more than 80+ Categories based on Application types, Security Risk level etc  |  |  |  |  |
| 3                          | Solution should support Application Detection and Usage Control.  |  |  |  |  |
| 4                          | Application Control Library should have more than 2000+ Web 2.0 applications and 200,000 Social Networking Widgets  |  |  |  |  |
| 5                          | Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc. ACTUAL (Application, Content, Time, User, Attack, Location)–based awareness capabilities |  |  |  |  |
| 6                          | Should have more than 500+ Categories based on Urls, Application types, Security Risk level etc   |  |  |  |  |
| 7                          | Application Control Databases should have sizable application and widget control list   |  |  |  |  |
| 8                          | Should have Categories like Business Applications, In-  |  |  |  |  |

|  |   |  |  |  |  |
|--|---|--|--|--|--|
|  | stant Messaging, File Page 37 of 67 Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Search Engine, Webmail etc . Should support User and Group based policies |  |  |  |  |
| 9  | Solution should have an option of creating custom categories for URL and Application control.   |  |  |  |  |
| 10   | Solution should have an option of mechanism of education users for eg Ask user before allowing access website   |  |  |  |  |
| 11   | Fine-grained identification of over 6000 application protocols, applicationspecific action, and online update of protocol databases   |  |  |  |  |
| 12   | Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications                       |  |  |  |  |
| 13   | Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks   |  |  |  |  |
| 14   | Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity                            |  |  |  |  |
| 15   | Real-time anti-spam to detect and filter out phishing emails  |  |  |  |  |
| <b>Administration, Management, &amp; Logging/Reporting Functionality</b> |   |  |  |  |  |
| 1  | Firewalls should be manageable from the centralized management framework.   |  |  |  |  |
| 2  | Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.  |  |  |  |  |
| 3  | The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.  |  |  |  |  |
| 4  | Firewall Real -Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance.   |  |  |  |  |
| 5  | Solution must provide hits against firewall rules to provide usability and information on utilization of rules in   |  |  |  |  |



|    |  |  |  |  |  |
|----|--|--|--|--|--|
|    | access Policy.   |  |  |  |  |
| 6  | Centralized management and reporting framework should be supplied as Hardware Appliance/Physical/Virtual Server  |  |  |  |  |
| 7  | Centralized management and reporting and appliance should have capability of minimum 2 TB storage capacity with provision for future expansion and should support 10GB logs per day capacity   |  |  |  |  |
| 8  | Any changes or commands issued by an authenticated user should be logged to a database.  |  |  |  |  |
| 9  | Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter. |  |  |  |  |
| 10 | The Firewall must provide simplified provisioning for addition of new firewalls where by a standard firewall policy could be pushed into the new firewall.   |  |  |  |  |
| 11 | Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.   |  |  |  |  |
| 12 | The Firewall administration station must provide a means for exporting the firewall rules set and configuration.   |  |  |  |  |
| 13 | Role based administration with multiple administrators should be supported   |  |  |  |  |
| 14 | The Firewall administration software must provide a means of viewing, filtering and managing the log data.   |  |  |  |  |
| 15 | The Firewall logs must contain information about the firewall policy rule that triggered the log.  |  |  |  |  |
| 16 | The centralized management solution should support integration with the Microsoft AD or LDAP to depict the user information in the collected log event for a better visibility   |  |  |  |  |
| 17 | The centralized management solution should be able to ingest the intelligence shared over STIX & TAXII from the SIEM solution  |  |  |  |  |
| 18 | Management framework and monitoring solution   |  |  |  |  |

|    |  |  |  |  |  |
|----|--|--|--|--|--|
|    | should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework including major regulations like ISO27001, PCI DSS, SOX etc.  |  |  |  |  |
| 19 | Management should provide detailed Event analysis for Firewall, IPS, Application Control, and DLP with reporting of all the components.  |  |  |  |  |
| 20 | Policy Management should have option to create various Layered policy for various Zones and should have option to create various Administrator to manage specific policy layers.   |  |  |  |  |
| 21 | Centralized management and Reporting Server/Appliance should have more than 10,000 logs/Sec processing capability  |  |  |  |  |
| 22 | Centralized management & Reporting solution should have internal redundant power supply (at least dual)<br><br>It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc. |  |  |  |  |
| 23 | It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.  |  |  |  |  |
| 24 | Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.  |  |  |  |  |
| 25 | All proposed components NGFW, Logging, Reporting etc should be managed from centralized management framework and if not then vendor need to provide additional components if any   |  |  |  |  |
| 26 | Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework  |  |  |  |  |
| 27 | Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc need to be provided with Real-Time and Historical reporting all the components.  |  |  |  |  |
| 28 | Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring  |  |  |  |  |



|                          |   |  |  |  |  |
|--------------------------|---|--|--|--|--|
|                          | various components of the appliance   |  |  |  |  |
| 29                       | The proposed system should be able to facilitate administration audit by logging detailed activities to event log for management, configuration changes, updates which also enable Admin to boot firmware on the earlier revision / configuration in case of any errors |  |  |  |  |
| 30                       | The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology. It should have network's physical and logical topology view  |  |  |  |  |
| <b>Certifications</b>    |   |  |  |  |  |
| 1                        | The Firewall should be ICSA Labs certified for Firewall, IPS, IPSec, SSL VPN  |  |  |  |  |
| 2                        | Security effectiveness should be recommended/certified by NSS labs  |  |  |  |  |
| 3                        | The Firewall should be EAL 4 + certified.   |  |  |  |  |
| 4                        | The resources to be deployed should have certification from the OEM for the product quoted  |  |  |  |  |
| 5                        | It should be NDPP certified, if not the same model  |  |  |  |  |
| <b>High Availability</b> |   |  |  |  |  |
| 1                        | System should have built-in high availability (HA) features without extra cost/license or hardware component  |  |  |  |  |
| 2                        | Should support state full session maintenance in the event of a fail-over to a standby unit.  |  |  |  |  |
| 3                        | High Availability feature must be supported for either NAT/Route or Transparent mode  |  |  |  |  |
| 4                        | Should support multiple heartbeat links   |  |  |  |  |
| 5                        | High Availability Configurations should support Active/Active, Active/ Passive & Clustering   |  |  |  |  |
| <b>Miscellaneous</b>     |   |  |  |  |  |
| 1                        | It should support different upload rates for different protocol packets to avoid the impact of the CPU by a large number of protocol packets and to protect the CPU.  |  |  |  |  |

|    |   |  |  |  |  |
|----|---|--|--|--|--|
| 2  | It serves as a proxy to detect and defend against threats in SSL-encrypted traffic using application-layer protection methods such as intrusion prevention, antivirus, data filtering, and URL filtering.                             |  |  |  |  |
| 3  | It allows users to create and manage virtual security services, including firewall, intrusion prevention, and antivirus services, on the same physical device.  |  |  |  |  |
| 4  | It automatically evaluates risks in security policies and provides tuning suggestions   |  |  |  |  |
| 5  | It should detect redundant and conflicting policies to remove unnecessary and incorrect policies  |  |  |  |  |
| 6  | Solution should support service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi homing scenarios.                   |  |  |  |  |
| 7  | It should identify common applications, supports application-specific access control, and combines application identification with intrusion prevention, antivirus, and data filtering to improve detection performance and accuracy. |  |  |  |  |
| 8  | It should secure direct Internet access for Cloud applications for improved latency and reduce WAN cost spending  |  |  |  |  |
| 9  | Management server should have capacity to manage at least 100 firewall devices  |  |  |  |  |
| 10 | The Firewall should support throughputs of 20 Gbps or better for both small & large packets   |  |  |  |  |

## Annexure VIII (Technical Approach & Methodology Document)

**N.B. :** Bidder is required to submit the Technical Approach & Methodology Document (TAMD) having the entire activity in details which would include but not limited to :-

- Scope of the project
- Detailed study of the existing setup
- Timeline
- Planning & Phasing
- Resources
- Tools ,if any
- Ensuring BCP & Measures to mitigate operational impact
- Measures to be taken in the event of an incident
- Escalation matrix
- Review Meetings etc

Annexure – IX Forwarding Letter (Commercial Bid)

**To,  
The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir,

With reference to Request for Proposal (RFP) Ref No. RFP No: \_\_\_\_\_ dated \_\_\_\_\_, I/we, the undersigned, offer to supply, deliver and commission the various requirements in conformity with the said RFP for the sum mentioned in the Price Bid or such other sums as may be ascertained in accordance with the Schedule of Prices attached and made part of this Bid. If our bid is accepted then :-

1. I/We undertake to deliver the goods and/or provide the services in accordance with the Delivery Schedule / implementation schedule specified.
2. If our bid is accepted, we will obtain the guarantee of a Bank in a sum equivalent to 10% per cent of the TCO for the due Performance of the Contract, in the form prescribed by NABARD.
3. We agree to abide by this bid during validity of the bid and may be accepted at any time before the expiration of that period.

WE FURTHER CONFIRM THAT,

1. Our offer is valid for a period of 180 days from the last date (revised last date if such date is extended by NABARD) for submission of the bid .
2. In case we offer system and/or other software manufactured by another company, such software operates effectively on the system offered by us and we are willing to accept responsibility for its successful operations.
3. Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your Notification of Award, shall constitute a binding Contract between us.
4. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
5. We understand that you are not bound to accept the lowest or any bid you may receive.

***(Signature)***

***(name & designation)***

***(Name & Address of the Bidder with Seal)***

## Annexure X (Commercial)

### A. Hardware and System Software Configuration Summary

| Sr. No.   | Item Name  | Description of your offer |
|-----------|--|---------------------------|
| <b>1.</b> | <b>Next Generation Firewall</b>                    |                           |
| 1.1       | Make of the Firewall                               |                           |
| 1.2       | Model of the Firewall                              |                           |
| 1.3       | Number of Ports                                    |                           |
| 1.4       | CPU Speed  |                           |
| 1.5       | Number of CPUs with above speed                    |                           |
| 1.6       | Minimum memory in each FireWall                    |                           |
| 1.7       | Space in each Firewall                             |                           |
| <b>2.</b> | <b>Management , Reporting &amp; Logging Server</b> |                           |
| 2.1       | Make of the Server                                 |                           |
| 2.2       | Model of the Server                                |                           |
| 2.3       | Number of Ports                                    |                           |
| 2.4       | CPU Speed  |                           |
| 2.5       | Number of CPUs with above speed                    |                           |
| 2.6       | Minimum memory in server                           |                           |
| 2.7       | Space in server                                    |                           |
| <b>3</b>  | <b>Switch</b>                                      |                           |
| 3.1       | Make of the switch                                 |                           |
| 3.2       | Model of the switch                                |                           |
| 3.3       | Number of Ports                                    |                           |
| 3.4       | Speed  |                           |

**(N.B. Please attach additional sheet for the detail of any other item other than mentioned above)**

### B. Cost/Price Matrix



**Table 1: Hardware for all NGFW components: -**

| Sl. No. | Make & Model | Part Code/Item Code etc. | No. of units | Base unit Cost | Tax | Total Cost | Remarks, if any |
|---------|--------------|--------------------------|--------------|----------------|-----|------------|-----------------|
| 1       |              |                          |              |                |     |            |                 |
| 2       |              |                          |              |                |     |            |                 |
| 3       |              |                          |              |                |     |            |                 |
| 4       |              |                          |              |                |     |            |                 |
| ...     |              |                          |              |                |     |            |                 |

**Table 2: Software/subscription/Licenses for all NGFW components: -**

| Sl. No. | Version & other details | Part Code/Item Code etc. | No. of units | Base unit Cost | Tax | Total Cost | Remarks, if any |
|---------|-------------------------|--------------------------|--------------|----------------|-----|------------|-----------------|
| 1       |                         |                          |              |                |     |            |                 |
| 2       |                         |                          |              |                |     |            |                 |
| 3       |                         |                          |              |                |     |            |                 |
| 4       |                         |                          |              |                |     |            |                 |
| ...     |                         |                          |              |                |     |            |                 |

**Table 3: One time Implementation Cost: -**

| Sl. No. | Item | Unit Cost | Tax | Total Cost | Remarks, if any |
|---------|------|-----------|-----|------------|-----------------|
| 1       |      |           |     |            |                 |
| 2       |      |           |     |            |                 |
| 3       |      |           |     |            |                 |
| 4       |      |           |     |            |                 |
| ...     |      |           |     |            |                 |

**Table 4: Warranty & Support (24X7) : -**

| Sl. No. | Items | Year Wise Warranty & Support/AMC Cost 24X7 |                 |                 |                 |                 | Total Cost | Remarks, if any |
|---------|-------|--|-----------------|-----------------|-----------------|-----------------|------------|-----------------|
|         |       | 1 <sup>st</sup>                            | 2 <sup>nd</sup> | 3 <sup>rd</sup> | 4 <sup>th</sup> | 5 <sup>th</sup> |            |                 |
| 1       |       |  |                 |                 |                 |                 |            |                 |
| 2       |       |  |                 |                 |                 |                 |            |                 |
| 3       |       |  |                 |                 |                 |                 |            |                 |
| 4       |       |  |                 |                 |                 |                 |            |                 |
| ...     |       |  |                 |                 |                 |                 |            |                 |





**Table 5: On-Site Support(8X5) :-**

| Sl. No. | Items | Unit Cost | Tax | Total Cost | Remarks, if any |
|---------|-------|-----------|-----|------------|-----------------|
| 1       |       |           |     |            |                 |
| 2       |       |           |     |            |                 |
| 3       |       |           |     |            |                 |
| 4       |       |           |     |            |                 |
| ...     |       |           |     |            |                 |

**Table 6 : Training Cost**

| Training type | No. of Tainee | No. of batches           | Cost | Tax | Total Cost |
|---------------|---------------|--------------------------|------|-----|------------|
| Administrator | 02            | Next Generation Firewall |      |     |            |

**C. Summary of the Cost (As applicable)**

| Sl.No. | Item       | Cost |
|--------|------------|------|
|        |            |      |
|        |            |      |
|        |            |      |
|        |            |      |
|        |            |      |
|        |            |      |
|        |            |      |
|        |            |      |
|        | <b>TCO</b> |      |

## Annexure XI (PBG)

### Proforma of "PERFORMANCE BANK GUARANTEE"

To

**The Chief General Manager**

**National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

In consideration of NABARD having Head Office at C-24, G-Block, Bandra-Kurla Complex, P.O. Box No.8121, Bandra (E), Mumbai – 400 051 hereinafter referred to as “Purchaser” is desirous of implementation of proposed Firewall solution along with creation of DMZ in the DC network at NABARD’s Head Office at Bandra-Kurla Complex, Mumbai and its various Regional offices (hereinafter referred to as “Services”) from M/s ----- (hereinafter referred to as “Contractor”) on the terms and conditions contained in their agreement/purchase order No ----- dt. ----- (hereinafter referred to as the “Contract”) subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the hardware, software, Warranty & Support, AMC, FMS, Training and associated components wrt the proposed firewall solution as per the terms and conditions of the said contract, to be supplied and rendered by the contractor and also guaranteeing the AMC & Training and other solution, along with associated components as per the terms and conditions of the said contract;

1) We, ----- (Bank) (hereinafter called “Bank”), in consideration of the premises and at the request of the contractor, do hereby guarantee and undertake to pay to the purchaser, forthwith on mere demand and without any demur, at any time up to ----- any money or moneys not exceeding a total sum of ₹.----- (Rupees ----- only) as may be claimed by the purchaser to be due from the contractor by way of loss or damage caused to or would be caused to or suffered by the purchaser by reason of failure of hardware, software, NGFW Solution, AMC, FMS, Training and associated components as per the terms and conditions of the said contract.

2) Notwithstanding anything to the contrary, the decision of the purchaser as to whether computer hardware and / or network solution and / or associated components have failed to perform as per the said contract, and also as to whether the contractor has failed to maintain the hardware, software, NG FW Solution, AMC, FMS, Training and associated components as per the terms and conditions of the said contract will be final and binding on Bank and Bank shall not be entitled to ask the purchaser to establish its claim or claims under this Guarantee but shall pay the same to the purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the contractor. Any such demand made by the purchaser on Bank shall be conclusive and binding notwithstanding any difference between the purchaser and the contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3) This Guarantee shall expire on -----; without prejudice to the purchaser's claim or claims demanded from or otherwise notified to Bank in writing on or before the said date i.e ----- (this date should be date of expiry of Warranty).

4) Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained purchaser shall be entitled to act as if Bank is the purchaser's principal debtors in respect of all the purchaser claims against the contractor hereby Guaranteed by the Bank as aforesaid and the Bank hereby expressly waive all its rights of suretyship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the purchaser that the purchaser shall have the fullest liberty without affecting in any manner Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the purchaser against the contractor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and Bank shall not be released from its liability for the reasons of any such extensions being granted to the contractor for any forbearance, act or omission on the part of the purchaser or any other indulgence shown by the purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the contractor or the Bank nor shall it be affected by any change in the constitution of the purchaser by any amalgamation or absorption or with the contractor, Bank or the purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by us (whether singly or jointly with other banks) on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing uncanceled and we further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by the Bank on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to the Bank's local address as mentioned in this guarantee.



10) Notwithstanding anything contained herein:-

i) Bank's liability under this Bank Guarantee shall not exceed ₹. ----- (Rupees-----  
---- only);

ii) This Bank Guarantee shall be valid up to -----;(date of expiry of Guarantee). and

iii) Bank is liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if the purchaser serve upon NABARD a written claim or demand on or before ----- (date of expiry of Guarantee Plus claim period of six months ).

11) Bank has power to issue this Guarantee under the statute/constitution and the undersigned has full power to sign this Guarantee on behalf of Bank.

**Date this ----- day of ----- 2014 at -----**

**For and on behalf of ----- Bank.**

**Sd/- -----**

## Annexure XII (EMD)

(Bank Guarantee in Lieu of EMD)

To

**The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir

WHEREAS the National Bank for Agriculture and Rural Development, a body corporate established under the NABARD Act, 1981 (hereinafter referred to as NABARD, which expression shall, include its successors and assigns) has invited tenders for "Next Generation Firewall" at its office at Bandra Kurla Complex, Bandra East, Mumbai

(2) WHEREAS M/s \_\_\_\_\_ who are our constituents (hereinafter referred to as "the Tenderers", which expression shall include the successors and assigns) have taken the tender for the said work.

(3) AND WHEREAS it is one of the condition of the said tender that the Tenderer shall deposit with the NABARD at the time of submitting the tender a sum of ₹.-----/- (Rupees -----only) as and by way of Bid Security (BS), which Bid Security (BS) shall not bear any interest and which shall be liable for forfeiture in the event of the Tenderer, after acceptance of his tender by NABARD, failing to observe any of the terms and conditions of the tender or the Tenderer not supplying the said license to the satisfaction of NABARD and / or its Consultants.

(4) AND WHEREAS at the request of the Tenderer, NABARD has agreed not to insist for payment of the said Bid Security (BS) in cash and accept the guarantee from a Scheduled Commercial Bank in lieu thereof and have agreed to accept the same from us, the Bank, as hereinafter contained.

In the premises aforesaid and in consideration of NABARD having agreed at our request to exempt the tenderer from depositing the said Bid Security (BS) in cash. WE, \_\_\_\_\_ Bank having our Head Office at \_\_\_\_\_ and one of our Branches at \_\_\_\_\_

Do hereby unconditionally and irrevocably guarantee unto the NABARD that the Tenderer will execute the Agreement soon upon acceptance of the tender by NABARD and will diligently, efficiently and satisfactorily perform all their obligations under the various terms and conditions of the said tender (read with any amendments made thereto by mutual consent of NABARD and the Tenderer) and supply the said license in the satisfaction of the NABARD / its Consultants within the time stipulated therein, failing which WE the \_\_\_\_\_ Bank shall, on demand and without demur, pay unto the NABARD the sum of ₹. -----/- (Rupees-----only) at its office at Mumbai.

We

\_\_\_\_\_ Bank further covenant that:

- (a) We shall pay the aforesaid sum on demand made in writing by NABARD without reference to the Tenderers and notwithstanding any dispute or difference that may exist or arise between the NABARD and the tenderers;
- (b) that this guarantee shall be a continuing guarantee and shall not be revoked by us without prior consent in writing of NABARD.
- (c) that the decision of NABARD on the breach of any of the terms and conditions of the said contract / tender by the Tenderers or their failure to perform their obligations or discharge their duties under the said tender / contract shall be final and binding on us and shall not be disputed by us inside or outside the court, tribunal, arbitration or other authority;
- (d) that the notice of demand in writing issued by NABARD shall be conclusive proof as regards the amount due and payable to NABARD under this guarantee and it shall not be disputed by us either inside or outside the court, tribunal or arbitration or other authority;
- (e) that any neglect or forbearance on the part of NABARD in enforcing any of the terms and conditions of the said tender / contract or any indulgence shown by NABARD to the Tenderer or any variation in the said tender / contract terms made by mutual agreement between NABARD and the Tenderer or any other act or deed on the part of NABARD which but for this clause may have the effect of discharging us under the law relating to guarantee / sureties shall not discharge us from our obligations herein and we shall be discharged only by compliance by the Tenderers with all their obligations / duties under the said tender / contract or by payment of the sum.
- (f) that this guarantee shall not be affected by any infirmity or absence or irregularity in the exercise of the powers by or on behalf of the tenderers to submit the said tender and enter into the said contract or any change in the constitution or dissolution of the Tenderers or change in its name;
- (g) that it shall not be necessary for NABARD to exhaust its remedies against the Tenderers before invoking this guarantee and the guarantee therein contained shall be enforceable against us notwithstanding any other security which the NABARD may have obtained or may hereafter be obtained from the Tenderers at the time when this guarantee is invoked is outstanding and unrealized;
- (h) that we hereby agree that this guarantee shall be valid and be in force for a period of Six months, i.e. upto \_\_\_\_\_ and we hereby agree to renew this guarantee for such further period or periods at the request of NABARD in the event of the works specified in the Tender are finally awarded to the Tenderers and / or the works awarded are not completed within the stipulated period and such renewal shall be entirely at the cost and expense of the Tenderer.
- (i) Any claim arising under this guarantee shall be preferred by NABARD within a period of six months from the aforesaid date of expiry i.e. \_\_\_\_\_ or, in the event of any renewal, within a period of six months from the date of expiry of such renewed period extended by such renewal, and unless the claim is so preferred against us, we shall stand discharged of all our liabilities hereunder.

***Yours faithfully***

***For and on behalf of***

\_\_\_\_\_ ***Bank***

***(Authorized Official)***



Annexure XIII (MAF)

**Manufacturer’s/Developer’s Authorization Form (MAF/DAF)**

*(To be filled for software application/ hardware/ system software/ RDBMS/ any other suites, whatsoever applicable separately)*

**To**

**The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir,

We \_\_\_\_\_ who are established and reputed manufacturer / developer of \_\_\_\_\_ having organization at \_\_\_\_\_ and \_\_\_\_\_ do hereby authorize M/s \_\_\_\_\_ (Name and address of Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above tender. We hereby extend our full guarantee and warranty for the following softwares / products offered by the above firm in response to NABARD’s tender and contract for supply, installation, commissioning, services and support for the Next generation Firewall as per the terms and conditions set out in the RFP document for the purpose.

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_

*(Please mention the names of the Softwares, Servers, System Softwares, RDBMS, and/or any other suites, as applicable).*

***Yours faithfully,  
(Name)***

***for and on behalf of  
M/s \_\_\_\_\_ (Name of Manufacturer/Developer)***

*Note: This letter of authority should be on the letterhead of the manufacturer(s) / developer(s) and should be signed by a competent person representing the manufacturer / developer.*

Annexure XIV (Back to Back Support)

**(Back To Back Warranty & Support)**

To

**The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir,

I/We \_\_\_\_\_ who are established and reputed manufacturer / developer of \_\_\_\_\_ having organization at \_\_\_\_\_ and \_\_\_\_\_ do hereby confirm that we will supply the listed items to M/s \_\_\_\_\_ for Next Generation Firewall Solution for NABARD.

I/We will provide back to back warranty & support wrt to all the items listed below.

I/We also confirm that in the event of M/s ..... not in a position to support NABARD's P3 level incident wrt the product then we would provide our best support.

SCHEDULE

*(Please indicate all the hardware/software)*

***Yours faithfully***

***(Name and Designation) of Authorised Official***

*Note: This letter of authority should be on the letterhead of the manufacturer(s) / developer(s) and should be signed by a competent person representing the manufacturer / developer.*



Annexure XV (Indemnity)**(Letter of Indemnity)****To**

**The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir

**Sale, Deployment, Customisation and Implementation of NGFW and Support therefor**

WHEREAS the National Bank for Agriculture and Rural Development, a corporation established under the National Bank for Agriculture and Rural Development Act, 1981 (hereinafter referred to as 'NABARD') has expressed desire to purchase and deploy hardware & software to be used in DC & DR for the various functions as per the Scope of Work hereunder written and which are hereinafter for brevity sake referred to as 'NGFW', subject to our furnishing declarations and indemnity as contained hereafter.

**NOW THEREFORE THIS LETTER OR INDEMNITY WITNESSETH THAT:**

We, the \_\_\_\_\_ Limited hereby declare and certify that we are the rightful owners/licenseses of the said solution offered for sale to NABARD and that the sale of the said solution to NABARD by us and the use thereof by NABARD does not infringe the property or other intellectual property or copy rights of any other person and that the same does not infringe the Copy of Rights Act, 1957 or any other Act for the time being in force.

We, the said \_\_\_\_\_ Limited hereby agree to indemnify and keep indemnified and harmless NABARD, its Officers, servants, agents and other authorised persons against any action that may be brought against us for infringement of the right of property or other intellectual property or copy rights in respect of the said systems package supplied by us to NABARD and will defend the same at our cost and consequences and will pay or reimburse NABARD, its officers, servants, agents and other authorised persons from all costs and other expenses that they may be put to or incur in that connection in accordance with the terms as provided for within the end User License Agreement that accompanies the said systems.

We, the said \_\_\_\_\_ Limited hereby also agree to indemnify and keep indemnified and harmless NABARD, its Officers, servants, agents and other authorised persons against



any third party claims in respect of any damages or compensation payable in onsequences of any accident or injury sustained or suffered by our employees or agents, or by any other third party resulting from or by any action, omission, or operation conducted by or on behalf of us and against any and all claims by employees, workmen, contractors, sub-contractors, suppliers, agent(s), employed, engaged, or otherwise working for us, in respect of any and all claims under the Labour Laws including wages, salaries, remuneration, compensation or like.

SCHEDULE

*(Please indicate all the hardware/software)*

***Yours faithfully***

***(Name and Designation) of Authorised Official***

## Annexure XVI (Confidentiality)

### **(Confidentiality Undertaking)**

**To,  
The Chief General Manager  
National Bank for Agriculture and Rural Development  
Department of Information Technology, Fifth floor, C Wing  
C-24, 'G' Block, Bandra-kurla Complex,  
P.B. No. 8121, Bandra (East),  
Mumbai - 400 051.**

Dear Sir

We acknowledge that during the course of bidding for Request For Proposal (RFP) floated for implementation of NGFW in National Bank for Agriculture and Rural Development (NABARD), we shall have access to and be entrusted with the Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to NABARD and its business that is provided to us pursuant to this Undertaking.

In consideration of you providing opportunity to us to bid, and for this purpose making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Undertaking), to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of our response to the RFP and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than the following :-
  - " To our partners / directors and employees who need to know such Confidential Information to assist with the bidding for RFP floated for implementation of NGFW across NABARD;
  - " With your prior written consent, such consent not to be unreasonably withheld;
  - " To the extent that such disclosure is required by law;
  - " To the extent that such disclosure is required by any Rule or requirement of any regulatory authority with which we are bound to comply; and
  - " To our professional advisors for the purposes of seeking advice. Such professional advisors will be informed of the need to keep the information confidential.
4. We shall not disclose or divulge any of the Confidential Information to any other client of \_\_\_\_\_(name of product vendor / implementation partner)



NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT

5. This Undertaking shall continue perpetually unless and to the extent that you may release it in writing and we shall be liable for any breach of the terms and conditions contained herein.
6. This Undertaking shall be governed by and construed in accordance with Indian Law and any dispute arising from it shall be subject to the exclusive jurisdiction of the Mumbai courts.

*Yours Sincerely*

***Signature and Stamp of Company***

***Authorised Signatory***

***Position:***

***Date:***

## Annexure XVII (NDA)

### Non - Disclosure Agreement

This agreement is made on this the---- day of -----, 2011 between **National Bank for Agriculture and Rural Development (NABARD)** a company incorporated in India under the provisions of The Companies Act, 1956 (Section 25) and having its registered office at **C-24, G Block, Bandra-Kurla Complex, Bandra (East) Mumbai-400 051** (Hereinafter referred to as "NABARD") which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

**AND**

\_\_\_\_\_ (**Name of Vendor**) and having its registered office at \_\_\_\_\_ which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

**WHEREAS:**

NABARD had floated a Request for Proposal for Vulnerability Assessment And Penetration Testing of their Information system & IT infrastructure and whereas \_\_\_\_\_ (**Name of Vendor**) has been, through an RFP process, selected as the successful Bidder and has been awarded this work.

During the course of VAPT \_\_\_\_\_ (**Name of Vendor**) and NABARD may disclose to each other certain information which may be proprietary and/or of confidential nature.

**NOW THEREFORE**

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

1. For purposes of this Agreement, "**Confidential Information**" means, with respect to either party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the present or potential business, operation or financial condition of or relating to the disclosing party (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the receiving party in violation of this Agreement); (ii) is lawfully acquired by the receiving party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the receiving party prior to its disclosure under this Agreement; (iv) was or is independently developed by the receiving party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case the party so required shall give the other party prompt written notice, where possible, and use reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable such other party to seek a protective order or other appropriate remedy at such other party's sole costs.
2. This Agreement does not obligate either party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring by one party on

the other party any rights, license or authority in or to the information provided.

3. Each party agrees and undertakes that it shall not, without first obtaining the written consent of the other, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both parties may disclose any Confidential Information to their Affiliates, directors, officers, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.

4. The receiving party shall use the same degree of care and protection to protect the Confidential Information received by it from the disclosing party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.

5. The disclosing party shall not be in any way responsible for any decisions or commitments made by receiving party in relying on the disclosing party's Confidential Information.

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

7. Both parties acknowledge that the Confidential Information coming to the knowledge of the other may relate to and/or have implications regarding the future strategies, plans, business activities, methods, processes and or information of the parties, which afford them certain competitive and strategic advantage. Accordingly neither party shall use the Confidential Information in a manner that will jeopardise or adversely affect in any manner such future strategies, plans, business activities, methods, processes, information, and/or competitive and strategic advantage of the disclosing party.

8. The parties hereto acknowledge and agree that in the event of a breach or threatened breach by the other of the provisions of this Agreement, the party not in breach will have no adequate remedy in money or damages and accordingly the party not in breach shall be entitled to injunctive relief against such breach or threatened breach by the party in breach.

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



10. If any dispute arises between the parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 by a panel of three arbitrators.

Each party will appoint one arbitrator and the two arbitrators so appointed will appoint the third or the presiding arbitrator. Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the parties.

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

12. This Agreement shall not be amended, assigned or transferred by either party without the written consent of the other party.

13. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third party.

14. This Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the parties with respect to the subject matter hereof. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement.

**IN WITNESS WHEREOF** the parties hereto have duly executed this Agreement as of the date and year written above.

**National Bank for Agriculture and Rural Development**

\_\_\_\_\_

\_\_\_\_\_  
**(Name of Vendor)**

Name:  
Designation:

Name:  
Designation:

## Annexure XVIII (Pre-Integrity Pact)

### **Pre Contract Integrity Pact**

#### **General**

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on \_\_\_\_\_ day of the month of \_\_\_\_\_ between, on one hand, National Bank for Agriculture and Rural Development (NABARD), represented by Shri \_\_\_\_\_ (hereinafter called the “BUYER”, which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s \_\_\_\_\_ represented by Shri \_\_\_\_\_, Chief Executive Officer (hereinafter called the “BIDDER/Seller” which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to procure (Name of the Stores/Equipment/Item) and the BIDDER/Seller is willing to offer/has offered the stores and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a body corporate established under NABARD Act, 1981 having its Head Office at Plot No.C-24, Block ‘G’, Bandra-Kurla Complex, Bandra (East), Mumbai.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

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

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

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

#### **Commitments of the BUYER**

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



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

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

2. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

### **Commitments of BIDDERS**

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

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

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

3.3 BIDDERS shall disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principles or associates.

3.4 BIDDERS shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator/authorized government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

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

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

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

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

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

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

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER either directly or indirectly is a relative of any of the officers of the BUYER, or alternatively if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filling of tender.

The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1986.

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

#### 4. Previous Transgression

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

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

#### 5. Earnest Money (Security Deposit)

5.1 While submitting the commercial bid, the BIDDER shall deposit an amount Rs. as Earnest Money/Security Deposit, with the BUYER through a Bank Draft or a Pay Order in favour of **National Bank for Agriculture and Rural Development** payable at Mumbai

5.2 The Earnest Money/Security Deposit in respect of unsuccessful bidders shall be returned within Four weeks, only after the successful completion of the Bid Process.

The Earnest Money Deposit of the successful Vendor/Bidder shall be released on receipt of the Performance Bank Guarantee.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

## **6. Performance Bank Guarantee**

The successful Bidder shall, at his own expense, deposit with the Chief General Manager, DIT, NABARD, Head Office, Mumbai within 30 days of the notice of award of the tender, a Performance Bank Guarantee from a schedule commercial bank, payable on demand in terms of clause 13 for an amount equivalent to 10% of the of the total order value of hardware and software in lieu of Retention Money Deposit for the due performance and fulfilment of the warranty/contract by the Bidder.

The Performance Bank Guarantee shall be denominated in INDIAN RUPEES only.

Without prejudice to the other rights of NABARD under the contract in the matter, the proceeds of the performance bank guarantee shall be payable to NABARD as compensation for any loss resulting from the Bidder's failure to complete its obligations under the contract. NABARD shall notify the Bidder in writing of the invocation of the right to receive such compensation indicating the contractual obligation(s) for which the Bidder is in default.

The Performance Bank Guarantee will be discharged only after a period of six months after the expiry of the warranty period of 3 (three) years after due performance of the obligations of the Bidder under the contract.

## **7. Sanctions for Violations**

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

- i. To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.
- ii. The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

- iii. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.
- iv. To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2%, higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with another contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.
- v. To encase Earnest Money Deposit and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.
- vi. To cancel all or any other contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.
- vii. To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.
- viii. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.
- ix. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.
- x. Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact

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

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

## 8. **Fall Clause**

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

## 9. **Independent Monitors**

9.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given).

9.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

9.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

9.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

9.5 As soon as the Monitor notices or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

9.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

9.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

9.8 The Monitor will submit a written report to the designated Authority of BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and should the occasion arise submit proposals for correcting problematic situations.

**The IEM for this project would be**

***Shri Debabrata Sarkar  
Mayfair Boulevard (Narayan Apt.)  
Flat No.701, Main Avenue Road  
Santacruz (West)  
Mumbai - 400054***

**10. Facilitation of Investigation**

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

**11. Law and Place of Jurisdiction**

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



12. **Other Legal Actions**

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

13. **Validity**

13.1 The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later in case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

13.2 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

14. The parties hereby sign this Integrity Pact at \_\_\_\_\_ on \_\_\_\_\_

BUYER

BIDDER

Name of the Officer

Chief Executive Officer

Designation

NABARD

Witness

Witness

1. \_\_\_\_\_

1. \_\_\_\_\_

2. \_\_\_\_\_

2. \_\_\_\_\_



### Annexure XIX (Reference Sites)

List of Customer(preferably BFSI/DFI) availed similar solution in last 3 Years

| SI No. | Name and complete Postal Address of the Customer | Name, Designation, Telephone, Fax, Telex Nos., e-mail address of the contact person | Brief Scope of work | Number of users | Kick –off date | Project completion | Present Status if not completed as on date | Remarks |
|--------|--|---|---------------------|-----------------|----------------|--------------------|--|---------|
| 1      |  |   |                     |                 |                |                    |  |         |
| 2      |  |   |                     |                 |                |                    |  |         |
| 3      |  |   |                     |                 |                |                    |  |         |
| ...    |  |   |                     |                 |                |                    |  |         |

N.B.:Kindly attach proof against each of the Work completion/satisfaction certificate

## Annexure XX (Detailed Specifications)

**Table 1: Details**

| Sr. No.   | Item Name  | Description of your offer |
|-----------|--|---------------------------|
| <b>1.</b> | <b>Next Generation Firewall</b>                    |                           |
| 1.1       | Make of the Firewall                               |                           |
| 1.2       | Model of the Firewall                              |                           |
| 1.3       | Number of Ports                                    |                           |
| 1.4       | CPU Speed  |                           |
| 1.5       | Number of CPUs with above speed                    |                           |
| 1.6       | Minimum memory in each FireWall                    |                           |
| 1.7       | Space in each Firewall                             |                           |
| <b>2.</b> | <b>Management , Reporting &amp; Logging Server</b> |                           |
| 2.1       | Make of the Server                                 |                           |
| 2.2       | Model of the Server                                |                           |
| 2.3       | Number of Ports                                    |                           |
| 2.4       | CPU Speed  |                           |
| 2.5       | Number of CPUs with above speed                    |                           |
| 2.6       | Minimum memory in server                           |                           |
| 2.7       | Space in server                                    |                           |
| <b>3</b>  | <b>Switch</b>                                      |                           |
| 3.1       | Make of the switch                                 |                           |
| 3.2       | Model of the switch                                |                           |
| 3.3       | Number of Ports                                    |                           |
| 3.4       | Speed  |                           |



**Table 1: Next Generation Firewall**

| S/N | Particular                                      | Min requirement   | Offered | Remarks, if any |
|-----|---|---|---------|-----------------|
| 1.  | Operating System                                | Latest & stable version   |         |                 |
| 2.  | Security Processing cores                       | 04  |         |                 |
| 3.  | Memory  | 16 GB upgradable upto 64 GB   |         |                 |
| 4.  | Storage   | 256 GB  |         |                 |
| 5.  | Interfaces                                      | 4 x 10-GbE SFP+,<br>8 x 1-GbE SFP,<br>8 x 1 GbE,<br>1 GbE Management, 1 Console |         |                 |
| 6.  | Firewall Throughput (Big Packet)                | 20 Gpbs   |         |                 |
| 7.  | IPS Throughput                                  | 4 Gbps  |         |                 |
| 8.  | TLS/SSL throughput                              | 2 Gbps  |         |                 |
| 9.  | Full DPI throughput                             | 4 Gbps  |         |                 |
| 10. | IPSec VPN throughput                            | 4 Gbps  |         |                 |
| 11. | SSL VPN Throughput                              | 2 Gbps  |         |                 |
| 12. | Application Control Throughput                  | 4 Gbps  |         |                 |
| 13. | AntiMalware throughput                          | 2 Gbps  |         |                 |
| 14. | Threat Protection Throughput                    | 2 Gbps  |         |                 |
| 15. | Firewall latency                                | Less than 10 Microseconds   |         |                 |
| 16. | No of ISPs to be supported for Link Aggregation | 3   |         |                 |
| 17. | Concurrent Sessions                             | 10,00,000   |         |                 |
| 18. | New connections per second                      | 50,000  |         |                 |
| 19. | Total no of users                               | 10,000  |         |                 |
| 20. | Firewall Policies                               | 10,000  |         |                 |
| 21. | Concurrent SSL VPN users                        | 500   |         |                 |
| 22. | No. of Client to Gateway IPSec VPNs             | 1000  |         |                 |
| 23. | No. of Gateway to Gateway IPSec VPNs            | 100   |         |                 |
| 24. | Route based VPN                                 | RIP, OSPF   |         |                 |
| 25. | Routing protocols to be supported               | BGP, OSPF, RIP, static routes, policy-based routing                             |         |                 |
| 26. | QoS   | Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking,          |         |                 |
| 27. | Authentication                                  | LDAP (multiple domains), XAUTH/RADIUS, SSO,                                     |         |                 |



|     |                           |   |  |  |
|-----|---------------------------|---|--|--|
|     |                           | Novell, internal user data-base, Terminal Services, Citrix, Common Access Card (CAC)            |  |  |
| 28. | Standards to be supported | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 |  |  |
| 29. | High Availability         | Active-Active, Active-Passive, Clustering   |  |  |
| 30. | NAT                       | 1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode                      |  |  |
| 31. | VLAN Interfaces           | 128   |  |  |
| 32. | Certifications            | ICSA, NSS Labs  |  |  |
| 33. | VoIP                      | Full H323-v1-5, SIP   |  |  |
| 34. | Encryption                | DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography                             |  |  |
| 35. | Key exchange              | Diffie Hellman Groups 1, 2, 5, 14v  |  |  |
| 36. | Virtual Domain (Min/Max)  | 10/100  |  |  |

**Table 2: Management, Reporting & Logging server**

| S/N | Particular           | Min requirement  | Offered | Remarks, if any |
|-----|----------------------|--|---------|-----------------|
| 1.  | Operating System     | Latest & stable version from last 01 year  |         |                 |
| 2.  | Memory               | 32 GB  |         |                 |
| 3.  | Processor            | Intel® Xeon® processor E5-2600 product family or equivalent                        |         |                 |
| 4.  | Chipset              | Intel C600 or equivalent   |         |                 |
| 5.  | Storage              | Min 2 TB   |         |                 |
| 6.  | Minimum Slots        | 2 PCIe slots   |         |                 |
| 7.  | Hard Drives          | 2.5" PCIe SSD, SAS SSD, SATA SSD, SAS (15K, 10K), nearline SAS (7.2K), SATA (7.2K) |         |                 |
| 8.  | Remote Management    | Yes  |         |                 |
| 9.  | Availability         | High   |         |                 |
| 10. | Cache                | Min 2.5 MB per core  |         |                 |
| 11. | Log storage capacity | 1 GB /day  |         |                 |

(NB: The datasheet of each of the product offered must be furnished along with the technical offer)

## Schedule – 1(List of Offices)

### Office-wise Users

| S/N | Regional Office / Training Establishment | Total Users |
|-----|--|-------------|
| 1.  | Arunachal Pradesh Reg. Office            | 8           |
| 2.  | Assam Regional Office                    | 90          |
| 3.  | A & N Regional Office                    | 9           |
| 4.  | Bihar Regional Office                    | 124         |
| 5.  | BIRD Bolpur                              | 12          |
| 6.  | BIRD Lucknow                             | 66          |
| 7.  | BIRD Mangalore                           | 20          |
| 8.  | Chattisgarh Regional Office              | 66          |
| 9.  | Goa Regional Office                      | 18          |
| 10. | Gujarat Regional Office                  | 121         |
| 11. | Haryana Regional Office                  | 86          |
| 12. | Head Office - Mumbai                     | 766         |
| 13. | H P Regional Office                      | 65          |
| 14. | Jharkhand Regional Office                | 74          |
| 15. | J & K Regional Office                    | 46          |
| 16. | Karnataka Regional Office                | 153         |
| 17. | Kerala Regional Office                   | 102         |
| 18. | Maharashtra Regional Office              | 172         |
| 19. | Manipur Regional Office                  | 9           |
| 20. | Meghalaya Regional Office                | 13          |
| 21. | Mizoram Regional Office                  | 8           |
| 22. | M P Regional Office                      | 124         |
| 23. | Nagaland Regional Office                 | 10          |
| 24. | New Delhi Regional Office                | 48          |
| 25. | Odisha Regional Office                   | 134         |
| 26. | Punjab Regional Office                   | 110         |
| 27. | Rajasthan Regional Office                | 133         |
| 28. | Sikkim Regional Office                   | 12          |
| 29. | Tamil Nadu Regional Office               | 164         |
| 30. | Telangana and AP RO                      | 157         |
| 31. | Tripura Regional Office                  | 12          |
| 32. | Uttarakhand Regional Office              | 59          |
| 33. | U P Regional Office                      | 193         |
| 34. | West Bengal Regional Office              | 139         |
|     | <b>Total</b>                             | <b>3326</b> |

(N.B.: The RO wise user figure indicated above may slightly differ due to transfers, recruitments & retirements etc.)

## Schedule – 2 (Location)

Location wise details of the same are as follows:

| S/N | Site                   | City       |
|-----|------------------------|------------|
| 1.  | Data Centre            | Mumbai     |
| 2.  | Disaster Recovery Site | Near Delhi |

## Schedule – 3 (Existing Firewalls & UTM)

List of existing firewalls/UTMs in the network

| Sl.No. | Existing Firewall /UTM | Location         | Make & Model |
|--------|------------------------|------------------|--------------|
| 1      | Checkpoint UTM         | Data Center      | CP 12400     |
| 2      | Checkpoint UTM         | Big & Medium ROs | CP 4400      |
| 3      | Checkpoint UTM         | Smaller ROs      | CP 1180      |
| 4      | SonicWALL              | Data Center      | NSA4500      |
| 5      | SonicWALL              | Disaster Center  | NSA3600      |

### Schedule 4 (Calculation Table)

**Example of Calculation to be adopted for arriving at L1**

| Bidder   | X                              | Y                                | Z                                |
|--|--------------------------------|----------------------------------|----------------------------------|
| (A) Technical Evaluation Marks                           | 85                             | 100                              | 95                               |
| Base is 100% of the highest scoring bidder               | 85                             | 100                              | 95                               |
| Calculation(i)   | $(85/100) \times 70 = 59.50$   | $(100/100) \times 70 = 70$       | $(95/100) \times 70 = 66.50$     |
| Marks (A) Out of 70                                      | 59.50                          | 70                               | 66.50                            |
| (B) Commercial evaluation Price in INR                   | 1000                           | 1100                             | 1200                             |
| Calculation (ii)   | $(1000/1000) \times 100 = 100$ | $(1000/1100) \times 100 = 90.90$ | $(1000/1200) \times 100 = 83.33$ |
| Base is 100% of the lowest bidder                        | 100                            | 90.90                            | 83.33                            |
| Calculation (iii)  | $(100/100) \times 30 = 30$     | $(90.90/100) \times 30 = 27.27$  | $(83.33/100) \times 30 = 24.99$  |
| Marks (B) Out of 30                                      | 30                             | 27.27                            | 24.99                            |
| Total Marks (A+B) Out of 100                             | 89.50                          | 97.27                            | 91.49                            |
| Ranking of Bidder  | L3                             | L1                               | L2                               |
| Hence, Y is the L1 bidder with highest cumulative marks. |                                |                                  |                                  |



Document Check List

| Sl.No. | Document | Enclosed (Yes/No) |
|--------|----------|-------------------|
| 1      |          |                   |
| 2      |          |                   |
| 3      |          |                   |
| 4      |          |                   |
| 5      |          |                   |
| 6      |          |                   |
| 7      |          |                   |
| 8      |          |                   |
| 9      |          |                   |
| 10     |          |                   |
| 11     |          |                   |
| 12     |          |                   |
| 13     |          |                   |
| 14     |          |                   |
| 15     |          |                   |
| 16     |          |                   |
| 17     |          |                   |
| 18     |          |                   |
| 19     |          |                   |
| 20     |          |                   |
| 21     |          |                   |
| 22     |          |                   |
| 23     |          |                   |
| 24     |          |                   |
| 25     |          |                   |
| 26     |          |                   |
| 27     |          |                   |
| ...    |          |                   |

End of Document

---