



(HEAD OFFICE: BANGALORE)

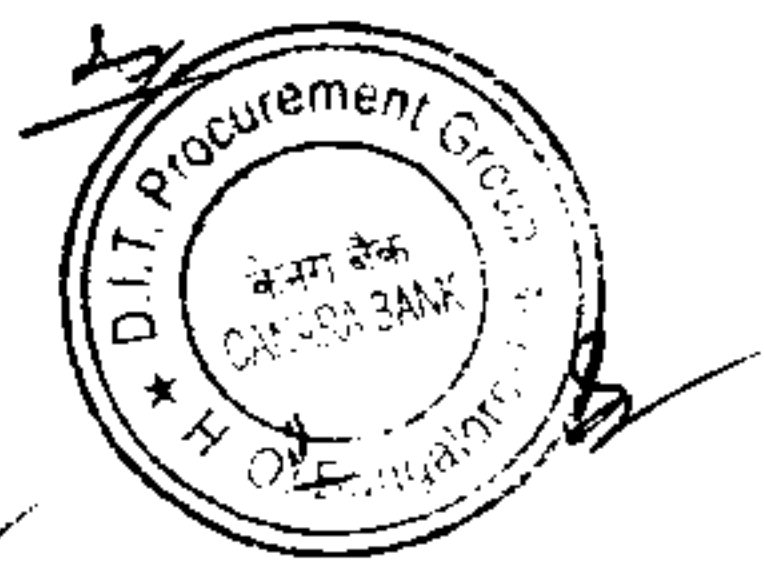
GLOBAL TENDER FOR  
IMPLEMENTATION OF  
ANTI-PHISHING, ANTI-PHARMING, ANTI-TROJAN, ANTI-MALWARE  
MANAGED SERVICES  
IN  
CANARA BANK

TENDER REFERENCE NO : RFP 06/2011-12  
DATE OF TENDER DOCUMENT : 08.06.2011  
DATE OF PRE BID MEETING : 17.06.2011, 03.00 PM  
LAST DATE FOR SUBMISSION OF TENDER : 08.07.2011 UPTO 3.00 PM  
DATE OF OPENING OF TECHNICAL BID PART A : 08.07.2011 AT 3.30 PM  
COST OF TENDER DOCUMENT : ₹ 5,000/- (Non Refundable)  
EARNEST MONEY DEPOSIT/BG IN LIEU OF EMD : ₹ 5,00,000/-  
NO. OF PAGES : 41 Pages

ISSUED BY : DEPUTY GENERAL MANAGER  
CANARA BANK  
ASSET PROCUREMENT & MANAGEMENT GROUP  
DIT WING, HEAD OFFICE  
NAVEEN COMPLEX, 14, M G ROAD  
BANGALORE 560 001

Contact Numbers : Tel-080-25599788  
Fax-080-25596539  
Email: [hoditapm@canarabank.com](mailto:hoditapm@canarabank.com)  
(Senior Manager, Asset Procurement & Management Group)

This document can be downloaded from Bank's website <http://www.canarabank.com/English/Scripts/Tenders.aspx>. In that event, the bidders should pay the cost of the tender document by means of DD drawn on any scheduled Bank for ₹ 5,000/- in favour of Canara Bank, payable at Bangalore and enclose the same to Technical Bid PART A of this tender.



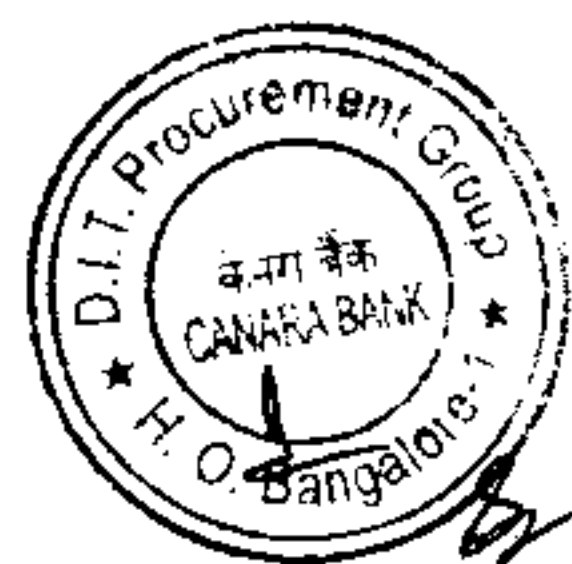
## CONTENTS

SL. NO.	DETAILS	PAGE NO.
	INTRODUCTION	4
	ELIGIBILITY CRITERIA	4-5
<b>1</b>	<b>INSTRUCTIONS</b>	<b>6-14</b>
1.1	BIDDERS RESPONSE & OPENING OF BID	6
1.2	REQUIREMENT DETAILS	8
1.3	DETERMINATION OF L-1 PRICE	8
1.4	TIME SCHEDULE	9
1.5	OFFER VALIDITY PERIOD	9
1.6	PROPOSAL OWNERSHIP	9
1.7	MODIFICATIONS AND WITHDRAWALS OF BID/S	9
1.8	PRE-BID MEETING	9
1.9	PRELIMINARY SCRUTINY	9
1.10	CLARIFICATION OF OFFERS	10
1.11	NO COMMITMENT TO ACCEPT LOWEST OR ANY OFFER	10
1.12	SUBMISSION OF TECHNICAL DETAILS	10
1.13	FORMAT FOR TECHNICAL BID	11-12
1.14	FORMAT FOR COMMERCIAL BID.	12
1.15	ERASURES OR ALTERATIONS	13
1.16	ALTERNATIVE OFFERS/BIDS	13
1.17	PRICE	13
1.18	EARNEST MONEY DEPOSIT	14
<b>2</b>	<b>TERMS AND CONDITIONS</b>	<b>14-19</b>
2.1	EFFECTIVE DATE	14-15
2.2	SCOPE OF WORK	15
2.3	DELIVERY, INSTALLATION, COMMISSIONING & ACCEPTANCE	15
2.4	UPTIME	15
2.5	LIQUIDATED DAMAGES	15-16
2.6	PENALTY	16
2.7	NON DISCLOSURE AGREEMENT	16
2.8	TERMS OF PAYMENT	16-17
2.9	PERFORMANCE BANK GUARANTEE	17
2.10	ORDER CANCELLATION / TERMINATION OF CONTRACT	17-18
2.11	LOCAL SUPPORT	18
2.12	INDEMNITY	18
2.13	PUBLICITY	18
2.14	GUARANTEES	18

2.15	NEGLIGENCE	18
2.16	RESPONSIBILIITY FOR COMPLETENESS	18-19
2.17	FORCE MAJEURE	19
2.18	RESOLUTION OF DISPUTES.	19
2.19	JURISDICTION	20
	<b>ANNEXURES</b>	
		21-41
A	SCOPE OF WORK	21-24
B	COVERING LETTER FORMAT	25-26
C	PARTICULARS OF BIDDER	27-28
D	TRACK RECORD OF PAST IMPLEMENTATION OF ANTI-PHISHING, ANTI-PHARMING, ANTI-TROJAN, ANTI-MALWARE MANAGED SERVICES	29
E	TECHNICAL COMPLIANCE STATEMENT	30
F	AUTHORIZATION LETTER FORMAT	31
G	MANUFACTURER'S AUTHORIZATION FORM	32
H	BILL OF MATERIAL AND PRICE SCHEDULE	33-34
I	TECHNICAL SPECIFICATIONS	36-39
J	BANK GUARANTEE FORMAT FOR EARNEST MONEY DEPOSIT	40-41

## CALENDER OF EVENTS

Sl. No	EVENT	DATE
1	Date of Issue	08.06.2011 Wednesday
2	Date of Submission of Queries for Pre Bid Meeting	13.06.2011 Monday
3	Date of Pre Bid Meeting	17.06.2011 Friday 03.00 PM
4	Date of Submission	08.07.2011 Friday 03.00 PM
5	Date of Opening of Technical Bid Part A	08.07.2011 Friday 03.30 PM
6	Date of Opening of Technical Bid Part B	Will be intimated subsequently
7	Date of opening of Commercial Bid	Will be intimated subsequently



**REQUEST FOR PROPOSAL (RFP) FOR IMPLEMENTATION OF ANTI-PHISHING, ANTI-PHARMING, ANTI-TROJAN, ANTI-MALWARE MANAGED SERVICES IN CANARA BANK**

**INTRODUCTION:**

Canara Bank is a premier Indian Public Sector Bank having Pan India presence with its operations spreading across length and breadth of the country.

Bank has launched transaction-based Internet Banking facility, through the Bank portal for providing online banking services to its retail and corporate customers on 24 x 7 basis with customer base more than 3.6 lacs and expected to grow exponentially.

To ensure that customers enjoy the complete benefits of these services and prevent customer's data going to the wrong hands, Bank is calling bids from the reputed, experienced and dynamic Service Providers and Original Equipment manufacturers (OEMs) to provide proactive monitoring of world wide web and blocking of cyber attacks / online frauds such as Phishing, Pharming, Trojans, Fraud Emails, Malwares, Brand Abuse, retrieval of compromised customer information and forensic details of such attacks and take down the sites and provide appropriate solution .

We invite sealed offers (Technical Bid and Commercial Bid) for implementing the Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services as described in this document.

A vendor submitting the proposal in response to this RFP shall hereinafter be referred to as 'Bidder'.

Interested Bidders who can offer and implement the Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in the Bank and meeting the following Eligibility Criteria may respond.

**ELIGIBILITY CRITERIA**

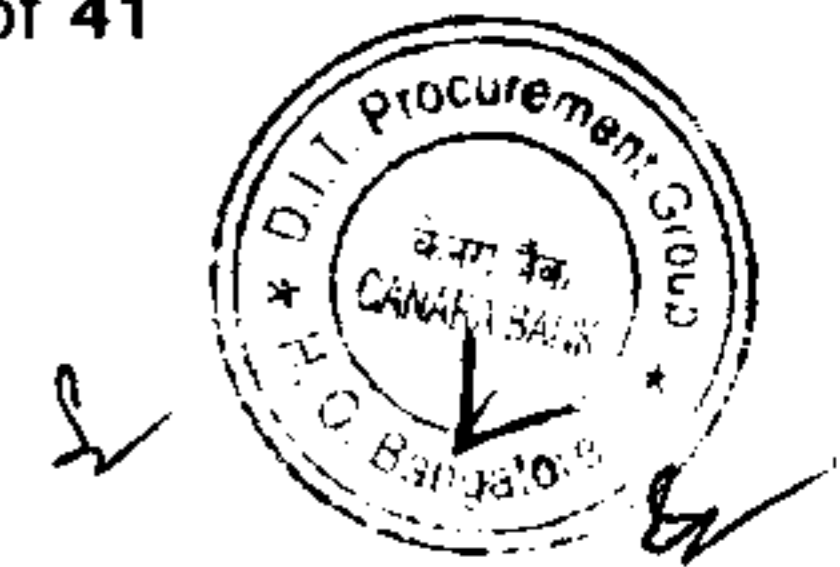
Sl. No	Criteria	Documents Required
1.	The Bidder is registered as a company in India as per Company Act 1956	Private Ltd Company: Copy of Certificate of Incorporation issued by the Registrar of Companies. Public Ltd Company : Copy of Certificate of Incorporation and Certificate of Commencement of Business issued by the Registrar of Companies.



2.	The bidder shall be the owner/certified or authorized agent / partner of the software solution offered.	If the bidder is not the solution owner, letter from the solution owner authorizing the bidder to participate in the tender to be enclosed.  Authorization letter from OEM as per Annexure G.  The declaration and Authorisation letter should not be older than six months earlier to the date of submission of Bid.
3.	Bidder must have a minimum turnover of Rs. 25.00 Crores per year during last three financial years i.e. 2007-08 and 2008-09, 2009-10 in IT related business in India.	Audited Balance Sheet and P & L Account for the last three years.  Certificate from Chartered Accountant certifying the IT related business turnover of last three years i.e. 2007-08, 2008-09 & 2009-10.
4	Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business (supply, integration, services, maintenance, audit etc)	Certificate from customers to be produced
5	Bidder should be registered / empanelled with Cert-in	Cert-In approved letter to be produced
6	The proposed services should have been provided by the bidder to at least one Public Sector Bank / Private Sector Bank in India in the last 2 years and the services must be currently running	Letter from the Bank to be produced for having successfully implemented.
7	Bidder should have minimum 5 CISA / CISM/ CISSP/ CIHE/ CVA/ CCSE security related certification holders in the organization	Profile of employees with certified copies.

Further, all bidders will have to submit the following:

1	Non Interest EMD for Rs.5,00,000/-	By way of DD favoring "Canara Bank" payable at Bangalore/Bank Guarantee.
2	Application fees for Rs. 5,000/- Non Refundable	By way of DD favoring "Canara Bank" payable at Bangalore



Failure to produce the documents as necessary proof along with the EMD and Application fee while submission of RFP proposal shall render the applicant ineligible for participating in the bid.

The bidder should submit separate DDs one each for EMD and Application Fee, if DDs are submitted.

Before submission of the offer, the Bidders are requested to go through the following instructions and the terms and conditions detailed below.

## **1. INSTRUCTIONS.**

### **1.1 BIDDER'S RESPONSE AND OPENING OF BIDS**

#### **1.1.1. Preparation of Bids**

1.1.1.1 The bidder has to submit the response to the bid in

- Technical Bid Part A - indicating their compliance to Eligibility Criteria as per Annexure B,C,D,E and G.
- Technical Bid Part B - indicating the response to the technical and functional requirement specifications of the Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services as per Annexure I.
- Commercial Bid - furnishing all relevant information as required in Bill of Material as Per Annexure H.

1.1.1.2 All the Bids shall be submitted in English Language in Font size 12 and above.

#### **1.1.2. Submission of Bids**

##### **1.1.2.1. Technical Bid Part A**

The Technical Bid Part A for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services Solution is to be sealed in a separate Envelope superscribed on the top of the cover as "Technical Bid for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services - Part A".

The Technical Bid Part A must contain EMD/ Bank Guarantee in lieu of EMD as per clause 1.18 of Instructions of this document.

##### **1.1.2.2. Technical Bid - Part B**

The Technical Bid Part B for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services is to be sealed in a separate Envelope superscribed on the top of the cover as "Technical Bid



for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services - Part B “.

1.1.2.3. The Technical Bid Part B should be complete in all respects and contain all information sought for, as per Annexure I. The Technical Bid should not contain any price information. The Technical Bid Part B should be complete and should cover all products and services.

1.1.2.4. Commercial Bid

The Commercial Bid for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services Solution is to be sealed in a separate envelope superscribed on the top of the cover as “Commercial Bid for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services”.

Commercial Bid shall be submitted as per Bill of Material and other terms and conditions of RFP on prices. The Commercial Bid should give all relevant price information as per Annexure H.

Under no circumstances the Commercial Bid should be kept in Technical Bid Covers. *The placement of Commercial Bid in Technical Bid covers will make bid liable for rejection.*

1.1.2.5. All the pages of Bid including Brochures should be made in an organized, structured, and neat manner. Brochures / leaflets etc. should not be submitted in loose form. All the pages of the submitted bids should be paginated with Name, Seal and Signature of the Authorized Signatory. Bids with eraser / overwriting/cutting are liable to be rejected. If required, the corrections can be made by scoring out entries and writing afresh and the authorized signatory should authenticate. Authorization letter for signing the Bid documents duly signed by Company’s Authorised signatory should be submitted

1.1.2.6. The separately sealed envelopes containing Technical Bids both Part A & B and Commercial Bid for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services shall be placed and sealed in another big envelope superscribed on the top of the envelope as “Offer for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in Canara Bank in response to RFP 06/2011-12 DT 08.06.2011”. The Name of the Bidder and Due date of the RFP is to be specified on the top of the envelope.

1.1.2.7. The bid/s should be deposited in the Tender Box kept at Canara Bank, DIT Wing, First floor, Naveen Complex, 14 M G Road, Bangalore - 560 001, on or before Friday, 8th July 2011, 3:00 PM. If last day of submission of bids is declared a holiday under NI Act by the Government subsequent to issuance of RFP the next working day will be deemed to be the last day for submission of the RFP. The Bid/s which is/are deposited after the said date and time shall not be considered. No offer will be accepted directly.



1.1.2.8. If any of the bidders or all the bidders who has responded the RFP are not present during the specified date and time of opening it will be deemed that such Bidder is not interested to participate in the opening of the Bid/s and the Bank at its discretion will proceed further with opening of the technical bids in their absence.

### 1.1.3. Opening of Bids

1.1.3.1. The Technical Bid Part A shall be opened in the presence of the Bidder's representative on Friday, 08th July 2011, at 3:30 PM at Canara Bank, Conference Hall, II Floor, Naveen Complex, 14 M.G Road, Bangalore 560001. Bidder's representative may be present in the venue well in time along with an authorization letter in hand for each bid opening under this RFP, as per the format (Annexure -I) enclosed and sign in Register of Attendance during opening of Technical Bid Part A.

1.1.3.2. The Bidders may note that no further notice will be given in this regard. Further, in case the bank does not function on the aforesaid date due to unforeseen circumstances or holiday then the bid will be accepted upto 3.00 PM on the next working day and bids will be opened at 3:30 PM at the same venue on the same day.

1.1.3.3. The Technical Bid Part - A submitted by the bidder will be evaluated based on the eligibility criteria stipulated. The Technical Bid Part B of only those bidders who qualified in Technical Bid Part A will be opened with due communication by the bank.

1.1.3.4. The Commercial Bid of only those bidders who qualified in Technical Bid Part B will be opened with due communication by the Bank.

## 1.2 REQUIREMENT DETAILS

This tender consists of following requirements.

Sl No	Item Details
1	Managed services for Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware including all the relevant activities as mentioned in the Scope of Work as per Annexure A and Technical Specifications as per Annexure I .

## 1.3 DETERMINATION OF L1 PRICE

1.3.1 The Commercial Bids as per Bill of Material (Annexure H) to be submitted by the bidders.

1.3.2 The Commercial Bid will be evaluated based on the Total Cost of Ownership (TCO) as per Bill of Material, i.e., Two year realtime online monitoring, take down/blocking of 200 attacks per year and Bench marking Bank's net banking sites inclusive of taxes. Basing on the TCO, Ranking of the Bidders will be determined.





#### 1.4 TIME SCHEDULE

The monitoring services for anti phishing, anti-pharming, anti-trojan, anti-malware scanning should start within **30 days** from the date of acceptance of Purchase Order or from the date of signing the contract agreement whichever is earlier.

The Delay in implementation will attract Liquidated Damages as per the terms and conditions (Point No.2.5)

#### 1.5 OFFER VALIDITY PERIOD

The Offer submitted and the Price quoted therein shall be valid for 15 Months from the date of declaration of successful bidder and for such further period as mutually agreed between the bank and successful bidder.

#### 1.6 PROPOSAL OWNERSHIP

The proposal and all supporting documentation submitted by the bidder shall become the property of the Bank.

#### 1.7 MODIFICATIONS AND WITHDRAWALS OF BID/S

No offer can be modified or withdrawn by a Bidder after submission of Bid/s.

#### 1.8 PRE-BID MEETING

1.8.1. A pre-tender meeting of the intending bidders will be held at **15.00 hours IST on Friday 17<sup>th</sup> June 2011** at Canara Bank, Conference Hall, II Floor, Naveen Complex, 14 M G Road, Bangalore - 560 001 to clarify any point/doubt raised by them in respect of this RFP. No separate communication will be sent for this meeting. All communications regarding points requiring clarifications and any doubts shall be given in writing to the Deputy General Manager, DIT Wing, HO Bangalore by the intending bidders before **14.00 hours IST on 13<sup>th</sup> June 2011**.

1.8.2. Authorized representatives of interested bidders shall be present during the scheduled time. The Bank shall clarify the queries during the pre-bid meeting and the replies along with the queries shall be uploaded in the Bank's website and no individual correspondence shall be made. No individual consultation shall be entertained. Bank will not consider any other queries raised by the bidder's representative during the pre-bid meeting without prior notice.



### 1.9 PRELIMINARY SCRUTINY

The Bank will scrutinise the Bid/s received to determine whether they are complete in all respects as per the requirement of RFP, whether technical documentation as required to evaluate the offer has been submitted, whether the documents have been properly signed and whether items are offered as per the tender requirements.

### 1.10 CLARIFICATION OF OFFERS

During the process of scrutiny, evaluation and comparison of offers, the Bank may, at its discretion, seek clarifications from all the bidders/any of the bidders on the offer made by them. The request for such clarifications and the Bidders response will necessarily be in writing and it should be submitted within the time stipulated by the Bank.

### 1.11 NO COMMITMENT TO ACCEPT LOWEST OR ANY OFFER

- 1.11.1. The Bank is not bound to accept the lowest or any tender or to assign any reason for non-acceptance. It also reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.
- 1.11.2. The Bank will not be obliged to meet and have discussions with any bidder and / or to entertain any representations in this regard.
- 1.11.3. The bidder including those, whose tender is not accepted shall not be entitled to claim any costs, charges, damages and expenses of and incidental to or incurred by him through or in connection with his submission of tenders, even though the Bank may elect to modify/withdraw the tender.

### 1.12 SUBMISSION OF TECHNICAL DETAILS

- 1.12.1. It is mandatory to provide the technical specifications and details in the exact format as mentioned in Annexure I of this tender.
- 1.12.2. The Offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of technical information as per the format given in the offer.
- 1.12.3. The Bank shall not allow / permit changes in the technical specifications once it is submitted.
- 1.12.4. The relevant product/solution information offered, printed product brochure, technical specification sheets, elaborated technical solution details, etc. should be submitted along with the Offer. Failure to submit this information along with the Offer could result in disqualification.





### 1.13 FORMAT FOR TECHNICAL BID

Please note that all the pages of the Bid document including Annexure submitted to the Bank should be made in the Bidder's letter head, paginated, neatly filed and duly signed by the Authorised Signatory with Company Seal.

#### 1.13.1. FORMAT FOR TECHNICAL BID PART A

The list of Documents to be submitted for Technical Bid Part A for this RFP is as follows:

- a. Index of the all documents submitted, with page numbers.
- b. Earnest Money Deposit (EMD)/ BG In lieu of EMD for ₹ 5,00,000/-.
- c. Demand Draft favouring Canara Bank drawn on Bangalore for ₹ 5,000/- towards cost of application. The Technical Bid Part A will be evaluated only for those bidders who submit EMD and Cost of application.
- d. Bidder's Covering letter. This should be as per Annexure B.
- e. Profile of the Company / Firm as per Annexure C.
- f. Write up on the Work Experience / Expertise in Implementation & Maintenance of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services.
- g. Power of Attorney / Authorisation letter signed by the Competent Authority with the seal of the bidder's company / firm in the name of the person signing the tender documents.
- h. Copy of Certificate of Registration / Certificate of Commencement of Business.
- i. Purchase order copies issued by the Major Clients in respect of Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services since 1.4.2007 till date of RFP (08.06.11) to establish that the Bidder has implemented the Solution in India during the last two years. (one purchase order from Public Sector Bank/Private Sector Bank is mandatory)
- j. Satisfactory working certificate from minimum 1 major clients as per Eligibility Criteria (4) for having implemented similar Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services.
- k. Annual Reports (Audited Balance Sheet and P&L account) of the bidder's company / firm for the last 3 years. i.e., for the year 2007-08, 2008-09 and 2009-10.



- l. Certificate from the Chartered Accountant certifying the turnover of last three years i.e., 2007-08, 2008-09 and 2009-10 from IT related business in India.
- m. Manufacturer / Dealer / Distributor certificate - Certificate from OEM/ manufacturer for proving 3 years experience.
- n. Track record of Past 3 years for implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services covering Name and addresses of major clients and email ids, telephone numbers (landline and mobile no), fax numbers of their contact executives etc. as per the Annexure D.
- o. Technical Compliance Statement as per Annexure E.
- p. Manufacturers Authorization Form as per Annexure G.

#### 1.13.2. FORMAT FOR TECHNICAL BID PART B

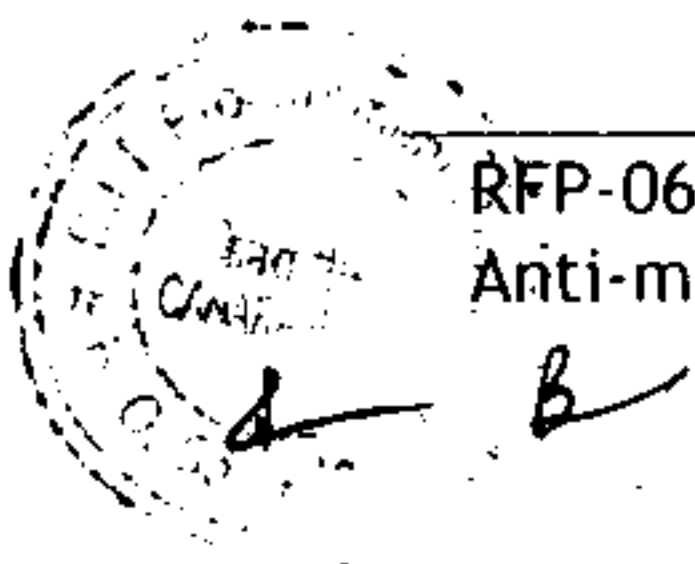
The list of Documents to be submitted for Technical Bid Part B for this RFP is as follows:

- a. The Bidder also to submit a certificate / letter from OEM of the Application software that the proposed Architecture offered by the bidder to the Bank are correct, viable, technically feasible for implementation and the solution will work without any hassles.
- b. Technical Offer as per Specifications given in Annexure I should be complete with all the columns filled in.
- c. The masked Price Offer should be enclosed to the Technical Offer as per Annexure H. This table should not contain any price information in Technical Offer.
- d. Technical Documentation (Product Brochures, leaflets, manuals, drawings). An index of technical documentation/solution submitted with the offer must be enclosed.
- e. A detailed list of the other Infrastructure hardware if any, required and any other precautions to be undertaken should be given in detail along with the Technical Bid.

#### 1.14 FORMAT FOR COMMERCIAL BID.

The Commercial Bid must not contradict the Technical Offer in any manner. The suggested format for submission of commercial Offer is as follows:

- a. Covering Letter
- b. Commercial Version of Bill of Materials and Price Schedule (as per Annexure-H).



### 1.15 ERASURES OR ALTERATIONS

The Offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled in. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "Accepted", "Noted", "As given in Brochure/Manual", "negotiable", "to be discussed" is not acceptable. The Bank may treat such Offers as not adhering to the tender guidelines and as unacceptable.

### 1.16 ALTERNATIVE OFFERS /BIDS

The Bidder/s desirous of offering the Bank two or more alternatives of Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services meeting the tender specifications should submit separate Offer/Bid for each alternative. Each alternative Offer /Bid should be complete in all respects and should not make cross-reference to details given in other offer/alternative. Every such alternative Offer should accompany separate EMD.

### 1.17 PRICE

- 1.17.1. The price should be quoted as per Bill of Material (BOM) -Annexure -H.
- 1.17.2. The Price/s quoted for implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in our Bank must be made in Indian Rupees only.
- 1.17.3. The Sales Tax / Value Added Tax / Central Sales Tax/ Entry Tax/ Octroi / Service Tax if any as applicable will be paid/reimbursed by the Bank at actual. Octroi /Entry Tax shall be reimbursed at actuals on submission of Original receipts.  
  
The Bidder should indicate the individual taxes, and its applicable rate along with the estimated tax amounts to be paid by the Bank.
- 1.17.4. If any of the deliverable product, mainly, Hardware, software, Service/Support etc. has both VAT and Service Tax, the bidder has to indicate the Goods component with percentage of VAT and Service Component with service Tax involved. The Goods Component + Service Component should be limited to 100% of the Cost Price, for example, if Goods Component is 60% then, the Service Component cannot be more than 40%.
- 1.17.5. If the bidder fails to include any other expenditure/item in the tender, no claim thereof will be considered by the bank afterwards.
- 1.17.6. No escalation in price is permitted for any reason whatsoever. Prices quoted must be firm till the completion of the contract including warranty period.
- 1.17.7. Bank shall place the Orders on the selected Bidder at cost price excluding tax.



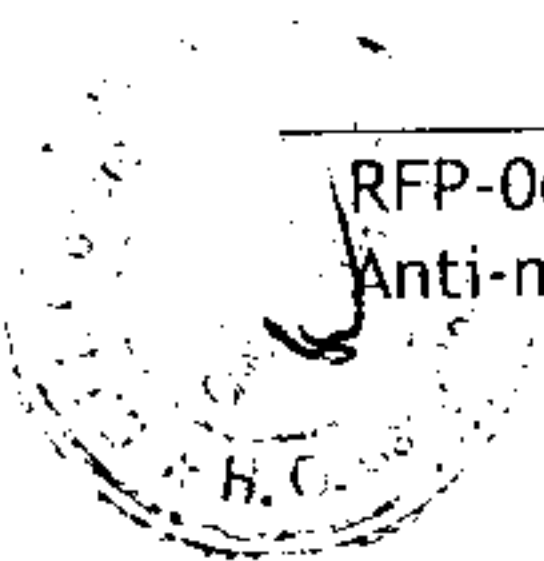
## 1.18 EARNEST MONEY DEPOSIT/BANK GUARANTEE IN LIEU OF EMD

- 1.18.1 The bidder shall submit Earnest Money Deposit (EMD) of ₹ 5,00,000/- (Rupees Five Lakhs only) by way of Demand Draft drawn on any scheduled Commercial bank in favour of Canara Bank, payable at Bangalore.
- 1.18.2 No interest is payable on EMD.
- 1.18.3 In Case, the EMD is submitted in the form of irrevocable Bank Guarantee, the same should be issued by any Scheduled Commercial Bank in India for ₹ 5 Lacs with a validity period of minimum 15 months from the last date for submission of offer. The format for submission of EMD in the form of Bank Guarantee is as per Annexure J.
- 1.18.4 The DD for EMD / Guarantee in lieu of EMD should be placed in the Technical Bid PART A only.
- 1.18.5 Submission of EMD / Bank Guarantee in lieu of EMD in other than Technical Bid PART A, is entirely at the risk of the bidder and in all such cases the bid is liable to be rejected on grounds of non submission of EMD.
- 1.18.6 The Technical Bid Part A will be evaluated only for those bidders who submit EMD/Bank Guarantee in lieu of EMD in the same cover.
- 1.18.7 The EMD of the Bidders not qualified under Technical Bid will be returned within 15 days after opening the commercial bid of the technically qualified bidders. The EMD of other bidders will be returned upon the selected bidder accepting the order and furnishing the performance guarantee.
- 1.18.8 For each alternative Offer/bid, a separate EMD/ Bank Guarantee in lieu of EMD must be submitted.
- 1.18.9 The EMD may be forfeited/ Bank Guarantee may be invoked:
  - 1.18.9.1 If the bidder withdraws or amends the bid during the period of bid validity specified in this document.
  - 1.18.9.2 If the selected bidder fails to accept the purchase order within 7 days or fails to sign the Contract Agreement or fails to furnish Performance Guarantee in accordance with the terms of the RFP.

## 2. TERMS AND CONDITIONS

### 2.1. EFFECTIVE DATE

- 2.1.1. The contract shall come into effect from the date of acceptance of Order by the successful bidder. Such acceptance shall be made within 7 days from the date of Order. The Project is deemed to have commenced from the date of acceptance of the Order by the Successful Bidder.



## 2.1.2. Execution of Agreement

- 2.1.2.1. Within 21 days from the date of acceptance of the Order by the selected Bidder, the selected bidder shall sign a stamped "Contract Agreement" with the Bank at the time, place and in the format prescribed by the Bank. Failure to execute the Contract Agreement makes the EMD liable for forfeiture at the discretion of the Bank and also rejection of the selected Bidder.
- 2.1.2.2. The Contract Agreement shall include all terms, conditions and specifications of RFP and also the Bill of Material and Price, as agreed finally after Bid evaluation and negotiation. The Contract shall be executed in English language in one original, the Bank receiving the duly signed Original and the selected Bidder receiving the photocopy. The contract shall be valid till all contractual obligations are fulfilled.

## 2.2. SCOPE OF WORK

The Successful Bidder has to carry out all the Scope of Works defined in Annexure-A and also to comply with the Technical Specifications narrated in Annexure-I and any other related works of this Project so as to ensure smooth implementation of Anti-phishing, anti-pharming, anti-trojan, anti-malware managed services Solution in Canara Bank.

## 2.3. DELIVERY, INSTALLATION, COMMISSIONING & ACCEPTANCE

- 2.3.1. The Bidder has to strictly comply with the Time Schedule.
- 2.3.2. The Bank will not arrange for any Road Permit / Sales Tax clearance for delivery of hardware, software, appliance to various locations and the Bidder has to make the arrangements for delivery of hardware, software, etc. to the locations as per the list of locations / items provided from time to time by the Bank.

## 2.4. UP-TIME

The managed services must have 100% uptime and shall be available on 24x7 basis.

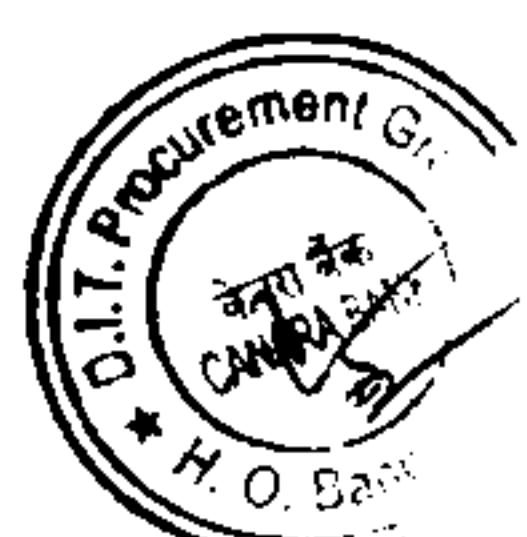
## 2.5. LIQUIDATED DAMAGES

The Bank will levy liquidated damages for the delay in adhering to the time schedule.

### 2.5.1.1. Liquidated damages for delay in implementation

If the bidder fails to complete implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in Bank as per the schedule 1.4 mentioned above, he shall be liable to pay as Liquidated damages at the rates specified below subject to a cap of 5%, for each completed calendar week of delay or part thereof, on the TOTAL PROJECT COST.

&



Liquidate Damages rate per week or part thereof	Delay Period
0.5% (Half Percent)	For the first Four weeks of Delay.
1.00 % (One Percent)	Beyond Four weeks of Delay.

2.5.1.2. The bidder agrees and considers that the liquidated damages set out herein above are fair and reasonable and that he will raise no objection or dispute with regard to the Bank's right to recover the liquidated damages.

2.5.1.3. The liquidated damages shall be deducted / recovered by the Bank from any money due or becoming due to the bidder under this purchase contract or may be recovered by invoking of Bank Guarantees or otherwise from bidder or from any other amount payable to the bidder in respect of other Orders.

2.5.1.4. All the above LDs are independent of each other and are applicable separately and concurrently.

2.5.1.5. LD is not applicable for the reasons attributable to the Bank and Force Majeure.

## 2.6. PENALTY

If the Selected Bidder fails to maintain response time (take down should happen within 4 hours from date and time of the anti phishing, anti pharming, anti malware scanning and anti Trojan incidents), penalty will be charged at the following rates -

Response time for > 8 hours but ≤ 12 hours	-	5% of quarterly payment
Response time for > 12 hours but ≤ 24 hours	-	10% of quarterly payment
Response time exceeding 24 hours	-	24% of quarterly payment

## 2.7. NON DISCLOSURE AGREEMENT

The successful bidder will have to execute a Non-disclosure agreement with the bank.

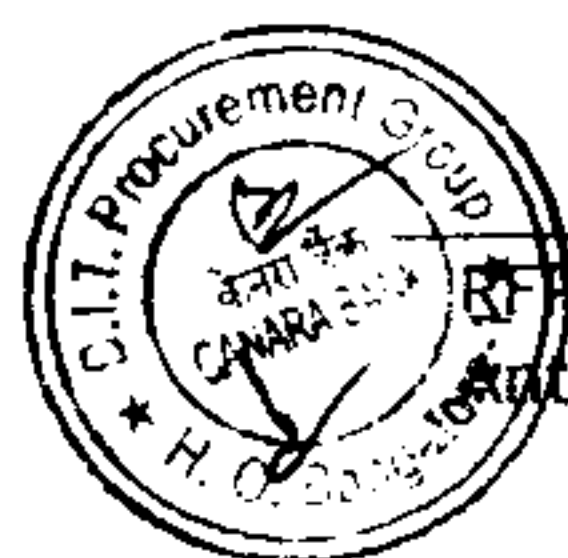
## 2.8. TERMS OF PAYMENT

The following terms of payment shall be applicable to this contract.

2.8.1 Bank will not pay any advance.

2.8.2 Payment will be made on quarterly in-arrears basis upon submission of proper invoices by the bidder duly certified by bank officials subject to "No pending issues" from bidder side.

- Period will be reckoned from the date commencement of the services.
- Bidder Company should raise proper invoices along with the proof of sites taken down/deactivated/blocked.



- c. Payment will be discharged after the Bank is satisfied of the services of the bidder company as per RFP at the end of the quarter after deducting applicable penalties and TDS.
- d. All payments will be made through RTGS/SFMS only.

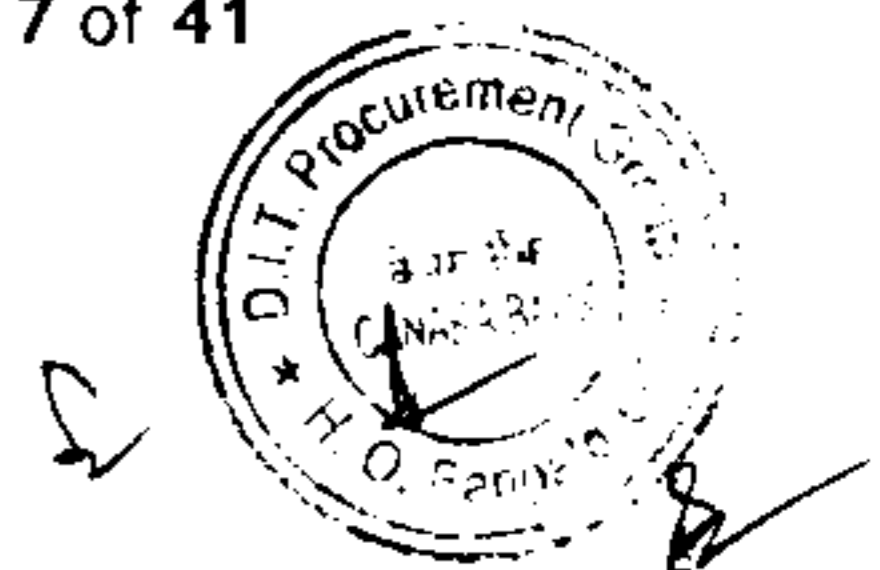
## 2.9. PERFORMANCE BANK GUARANTEE

- 2.9.1. The successful bidder should submit a Performance Bank Guarantee for **10% of total value of the contract within fifteen days** from the date of acceptance of the order.
- 2.9.2. If the Performance Guarantee is not submitted within the date stipulated, penalty at 0.50% per week or part thereof, on the value of the order will be deducted from the delivery payment for the delay in submission of Performance Guarantee.
- 2.9.3. The successful bidder should submit Performance Bank Guarantee issued by a First Class Scheduled Bank in India.
- 2.9.4. The Performance Bank Guarantee should be valid for 18 months. The guarantee should also contain a claim period of three months from the last date of validity.
- 2.9.5. The selected bidder shall be responsible for extending the validity date and claim period of the bank guarantees as and when it is due, on account of delay in completion of the project and warranty period.
- 2.9.6. The Bank shall invoke the Bank guarantee before the expiry of validity, if work is not completed and the guarantee is not extended, or if the selected bidder fails to complete his obligations under the contract. The bank shall notify the selected bidder in writing before invoking the bank guarantee. The proceeds of the guarantee shall be payable to the bank as compensation for any loss from the selected Bidder's failure to complete his obligations under the contract.

## 2.10. ORDER CANCELLATION / TERMINATION OF CONTRACT

The Bank reserves its right to cancel the entire / unexecuted part of Purchase Order at any time by assigning appropriate reasons in the event of one or more of the following conditions:

- i. Delay in Implementation of the Project beyond the specified periods.
- ii. Non satisfactory performance of the Project during Pilot implementation.
- iii. Failure to integrate / implement the project as per the requirements of the Bank.
- iv. Serious discrepancies noted in the implementation of the project
- v. Breaches in the terms and conditions of the Order.
- vi. Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/Offices of the Bank.



In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Performance Bank Guarantee given by the bidder towards non performance/non compliance of the terms and conditions of the contract, to appropriate the damages.

In the event of termination of contract, bank shall have the right to avail the services of any other person for the purpose without any let or hindrance from the successful bidder besides claiming the liquidated damages as per para 2.5.

#### 2.11. LOCAL SUPPORT

The Bidder should be capable of meeting the service & support standards as specified in this tender. Service support should be available on all Bank working days/ hours.

#### 2.12. INDEMNITY

The Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services supplied by them.

#### 2.13. PUBLICITY

Any publicity by the Bidder in which the name of the Bank is to be used will be done only with the explicit written permission of the Bank.

#### 2.14. GUARANTEES

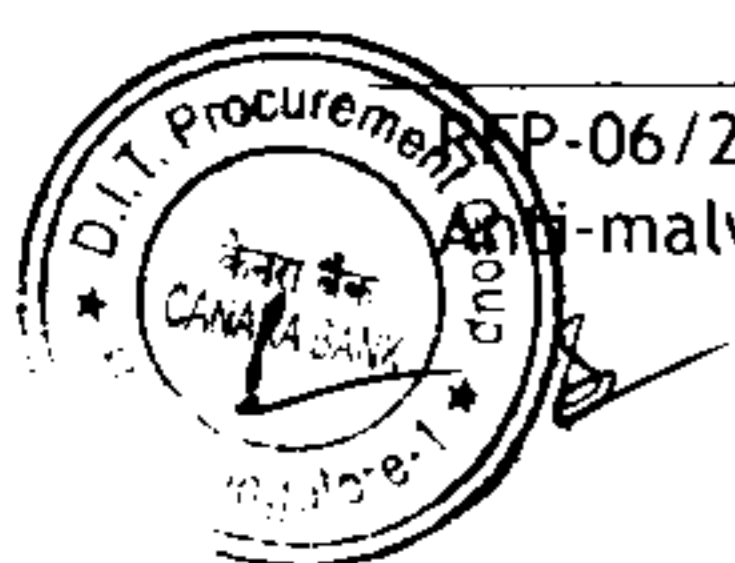
The Bidder should guarantee that the hardware delivered for Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services to the Bank are brand new, including all components if any. In the case of software, the Bidder should guarantee that the software supplied to the Bank includes all patches, upgrades / updates etc., and the same are licensed and legally obtained. All hardware and features must be supplied with their original and complete printed documentation.

#### 2.15. NEGLIGENCE

In connection with the work or contravenes the provisions of General Terms, If the Contractor neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the Contractor calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the Contractor liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the Contractor.

#### 2.16. RESPONSIBILTY FOR COMPLETENESS

Any supplies and services which might not have been specifically mentioned in this tender but are necessary for the design, engineering, manufacture, supply, installation,



testing, commissioning, performance or completeness of the order, shall be provided / made available as per the time schedule for smooth and efficient operation and maintenance of the system under Indian condition.

The Bidder shall be responsible for any discrepancies, errors and omissions in the drawings or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The bidder shall take all corrective measures arising out of discrepancies, error and omission in drawings and other information as mentioned above within the time schedule and without extra cost to the bank.

## 2.17. FORCE MAJEURE

The Bidder shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the Bidder, i.e. Force Majeure.

For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the Bidder, due to or as a result of or caused by acts of God, wars, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the Bidder, resulting in such a situation.

In the event of any such intervening Force Majeure, the Bidder shall notify the Bank in writing of such circumstances and the cause thereof immediately within five days. Unless otherwise directed by the Bank, the Bidder shall continue to perform / render / discharge other obligations as far as they can reasonably be attended / fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the Bidder shall hold consultations with each other in an endeavor to find a solution to the problem. Notwithstanding above, the decision of the Bank shall be final and binding on the Bidder.

## 2.18. RESOLUTION OF DISPUTES

All disputes and differences of any kind whatsoever, arising out of or in connection with this Offer or in the discharge of any obligation arising under this Offer (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably. In case of failure to resolve the disputes and differences amicably the matter may be referred to a sole arbitrator mutually agreed upon after issue of at least 30 days notice in writing to the other party clearly setting out their in the specific disputes. In the event of absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators; one to be nominated by each party and the said arbitrators shall appoint a presiding arbitrator. The provisions of the Indian Arbitration and Conciliation Act, 1996, shall govern the arbitration.

The venue of arbitration shall be Bangalore, INDIA.



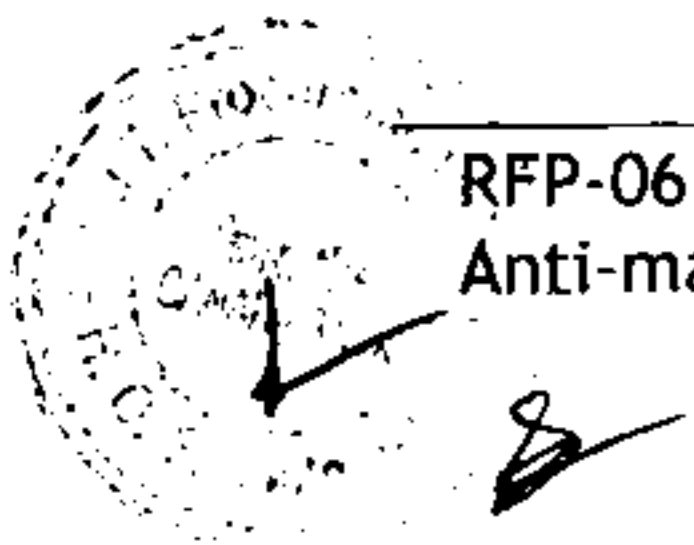
**2.19. JURISDICTION**

The Purchase Contract / Annual Maintenance Contract shall be governed by the Laws and Regulations of India for the time being in force and will be subject to the exclusive jurisdiction of the Courts in Bangalore, India.

Yours faithfully,



R Rajendran  
Deputy General Manager



ANNEXURE - A

Scope of Work

1. Objective:

The broad scope of work for the bidder under this RFP shall be

2. Purpose:

2.1. Bank has launched transaction-based Internet Banking facility, through the Bank portal for providing online banking services to its retail and corporate customers on 24 x 7 basis with customer base more than 3.6 lacs and expected to grow exponentially.

2.2. To ensure that customers enjoy the complete benefits of these services and prevent customer's data going to the wrong hands, Bank is calling bids from the reputed, experienced and dynamic Service Providers and Original Equipment manufacturers (OEMs) to provide proactive monitoring of world wide web and blocking of cyber attacks / online frauds such as Phishing, Pharming, Trojans, Fraud Emails, Malwares, Brand Abuse, retrieval of compromised customer information and forensic details of such attacks and take down the sites and provide appropriate solution .

3. Requirements & Scope of Work:

The proposed solution should have the following General Features:

Bidder will have to provide the following services for a period of two years as per the scope given below:

**Monitoring Internet and Identification of Remedies for Phishing, Pharming, Trojans, Spyware etc**

3.1. Bidder should be able to proactively monitor, detect and handle the following incidents (for the websites mentioned in the table given below).

- Phishing attempts
- Pharming attempts
- Trojans
- Malware
- Brand abuse cases
- Spoofed email ids that may be used for sending mails to the customers of the Bank.
- Monitoring of compromised servers for forensic information related to Bank's customers till the primary incident is closed.

3.2. Bidder should be able to handle proactively all kinds of frauds and simultaneously update itself with new frauds that may keep on coming. Bidder will have to provide



countermeasures/solutions for all existing frauds as well as frauds that may come in the near future.

- 3.3. Bidder should be able to provide 24\*7 support facility to the Bank for all activities that fall under the technical table of RFP.
- 3.4. Bidder should be capable to provide DR set up in case of any failure and must have a DR plan ready which is acceptable to the Bank.
- 3.5. Bidder should be able to report incident through all modes of communication that should include email, phone calls, SMS and dashboard. Details of compromised accounts should be shared immediately with the Bank.
- 3.6. Bidder should have the capability to ensure fast closure of the incident. Contacts with Browser vendors, ISP (Internet Service Provider) and third parties are a must in this case.
- 3.7. In case any account is compromised, proper tracking and reporting of fund is mandatory. The bidder has to assist the bank in case of legal case being raised by the customers for all such cases
- 3.8. Implementation of tools for referrer log analysis of web server
- 3.9. Monitoring similar domain name registrations
- 3.10. Monitoring of spam traps to detect phishing mails
- 3.11. Web site analysis to detect phishing sites
- 3.12. The Bidder should have alternative response mechanism other than web site take down to minimize impact of phishing
- 3.13. Assistance to bank in identifying customers affected by phishing, Pharming, malware, Trojan attacks.
- 3.14. Monitoring Brand abuse cases.
- 3.15. Blocking of the phishing sites for Browsers like Internet Explorer, Firefox, Chrome
- 3.16. Bidder should have trained staff who can provide support in all the language mentioned in the technical table.
- 3.17. Bidder should be able to provide legal support to the Bank in the form of communication with CERT/Cyber Crime Cells (with specific permission from the Bank). Technical support must be available to the Bank all the time.
- 3.18. Bidder should be able to provide a customized dashboard to the Bank that should include reports, help menu, downloading extracted data, availability of screen shots. Features should be included as mentioned in the technical table of RFP.

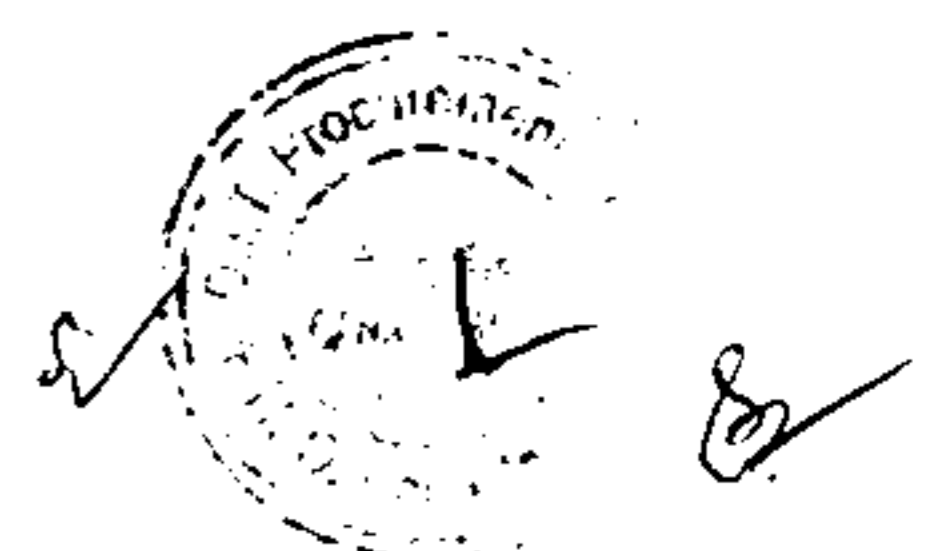


- 3.19. Bidder should have forensic capability to ensure the following functionalities:
- Comprehensive analysis of the incident
  - Extraction of critical data found during investigation and analysis
  - Store data for any future reference
- 3.20. Bidder should be able to provide advisory services to the Bank in the form of
- Advisories on online threats
- White papers
  - Information on critical vulnerabilities
  - Review calls
  - Intelligence alerts
  - Presentations
- 3.21. Bidder should meet all the security aspects highlighted in the technical table.
- 3.22. Bidder should meet all the parameters defined in SLA (to be executed upon selection) and maintain consistent performance.
- 3.23. Bidder should ensure that the analysis conducted for any incident must support the following.
- Underground intelligence analysis
  - Correlation of all attacks and underground intelligence
  - Capability to share and disseminate information on fraud related activities with members (May be a part of information sharing network such as Internet Relay Chat, Anti Phishing Work Group)
  - Intelligence gathered should be coordinated and collaborated with other intelligence gathering groups / teams / organizations
- 3.24. Bidder should ensure that these services must have the capacity to integrate in real time with knowledge based authentication solution.

Bidder should give the quote for a block of 200 incidents per annum. If the number of incidents exceeds the block of 200, such incidents in excess of the block of 200 should be considered on per incident basis and at the same rate that works out from the rate quoted for block of 200 incidents.

In case of phishing and Pharming incidents, if the same incident becomes active on the same server within a period of 90 days of its previous closure, it should not be treated as a new incident.

The scope of the services is to be provided for the period of 2 years from the date of initiation of respective service / solution (Services will be deemed to have been implemented from the **date of written confirmation by the bidder to this effect** and the solution will be deemed to have been implemented from the date of successful completion of User acceptance test).



**4. Other Conditions/Requirements:**

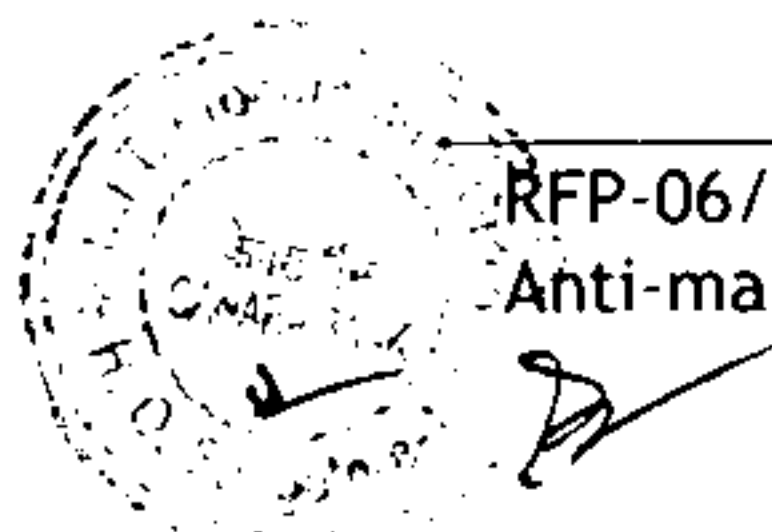
- 4.1. Bank reserves the right to extend the period of services for another one year or part thereof at the same terms and conditions.

**5. Security Policy.**

- 5.1. Anti-phishing, anti-malware, anti-pharming and anti-trojan managed services policy should be implemented based on Bank's security policy.

**GENERAL**

1. The Vendor to take always proactive, reactive, preventive and corrective maintenance steps and ensure that the functioning of the Bank is no way affected.
2. Designate one Senior Official for single point of contact by the Bank.
3. The Bidder should ensure that CBS & Other related Applications should run Smoothly during implementation and after implementation of this solution.
4. Vendor to ensure that the RISK & THREAT TO THE IT SYSTEMS OF THE BANK THROUGH VIRUSES, MALWARE & OTHER VULNERABLE ITEMS are minimized /curtailed and increase the security in IT area within our Banking System by implementing this solution.
5. At all points of time vendor should integrate, coordinate with all our System Integrators (SI) for smooth implementation.



**ANNEXURE - B**

[Note: This Covering letter should be on the letter head of Bidder and should be signed by a an Authorised Signatory with Name and Seal of the Company]

**Covering letter format**

Offer Reference No:

Date:

To

The Deputy General Manager,  
Canara Bank,  
Asset Procurement & Management Group,  
Department of Information and Technology,  
Naveen Complex, 14 M G Road,  
Bangalore - 560 001  
Karnataka

Dear Sir,

**Tender Ref: RFP- 06/11-12 DT: 08.06.2011**

Having examined the tender document including all AnnexureS, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to implement Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware Managed Services at Canara Bank in conformity with the said tender in accordance with the schedule of prices indicated in the commercial offer and made part of this offer.

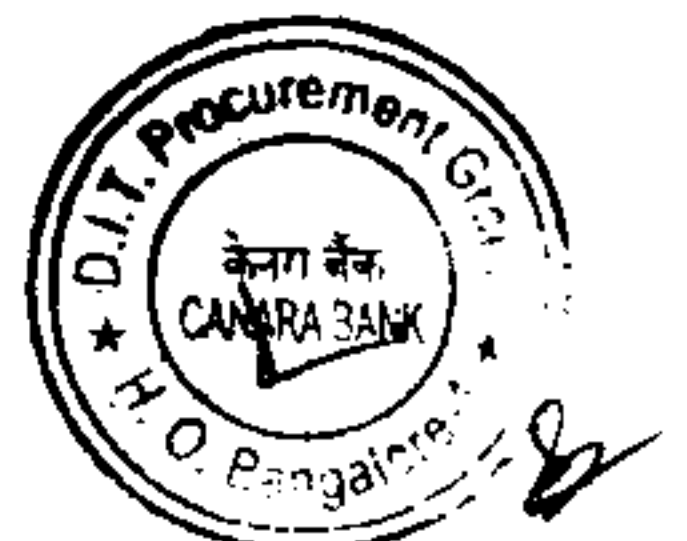
If our offer is accepted, we undertake the Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services project to the Bank within 30 days from the date of purchase order.

If our offer is accepted, we shall carry out all the works specified in Scope of Work (Annexure A) and also all other works related to implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in Bank.

We enclose a Demand Draft /Bank Guarantee in lieu of EMD for ₹ 5,00,000/- in favour of Canara Bank as EMD.

We also enclosed a DD for Rs. 5,000/- in favor of Canara Bank towards cost of application.

We agree to abide by this offer till 15 months from the date of declaration of successful Bidder and for such further period as may be requested for by the Bank, and agreed to in writing by the bidder. We also agree to keep the Earnest Money Deposit/Bank Guarantee in lieu of EMD during the entire validity period of the tender. However if we withdraw our offer within the said validity period, you shall have the right to forfeit the EMD/invoke the Bank Guarantee in lieu of EMD, without



reference to us. We agree to abide by and fulfill all the terms and conditions of the tender and in default thereof, to forfeit and pay to you or your successors, or authorized nominees such sums of money as are stipulated in the conditions contained in tender together with the return acceptance of the contract for implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services.

We enclose a list of clients in India (giving their full addresses) where we have implemented Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services.

Our PAN number for Income Tax is \_\_\_\_\_.

We are registered with the Sales Tax/Service Tax authorities and our registration numbers are as follows.

Sales Tax/VAT Registration Number is \_\_\_\_\_.

Service Tax Registration Number is \_\_\_\_\_.

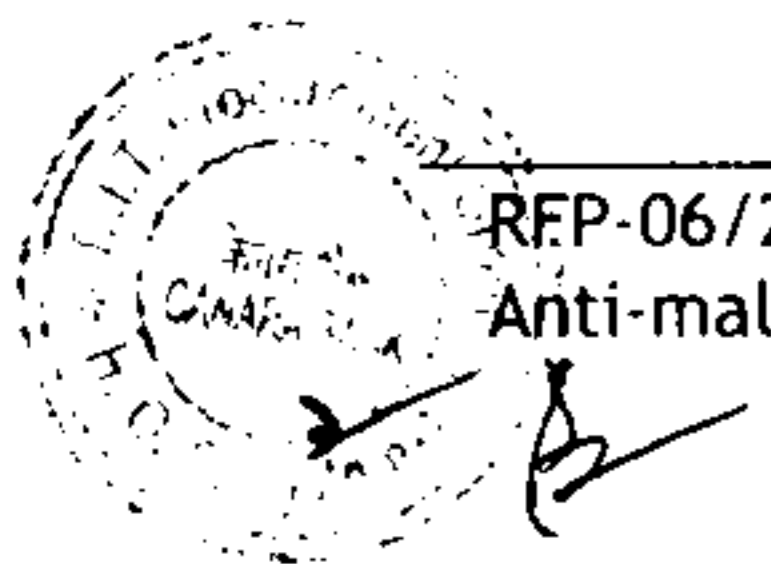
We accept all the Instructions and Terms and Conditions of the subject RFP.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive without assigning any reason whatsoever.

Dated this \_\_\_\_\_ day of \_\_\_\_\_ 2011

Signature \_\_\_\_\_

**Signature of the Authorized Signatory with date & seal**

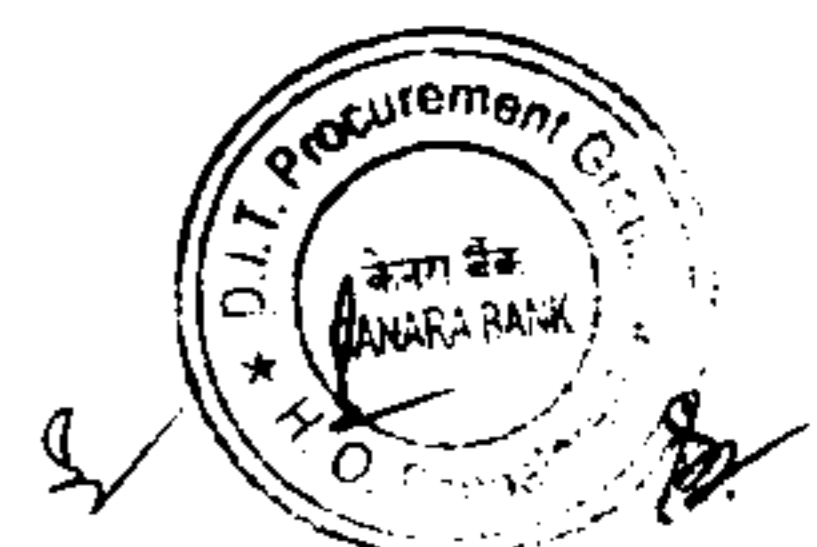




**ANNEXURE - C**

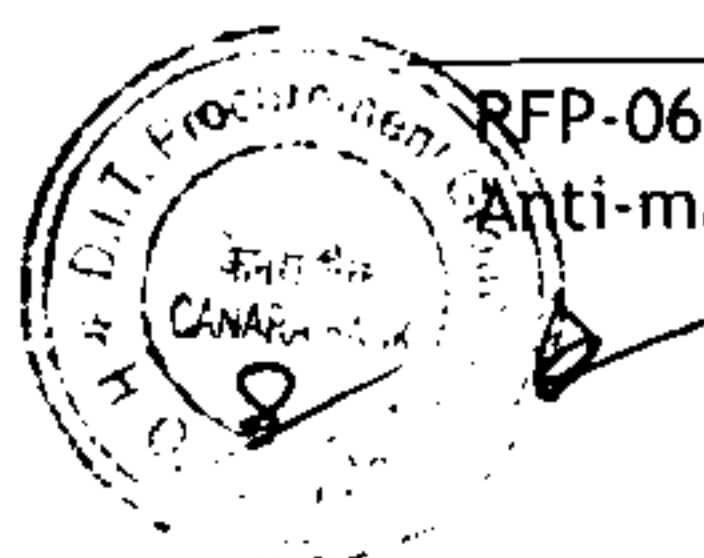
**Particulars of Bidder**

Sl. No	Particulars	
<b>A</b>	<b>Company/Bidder Profile</b>	
1	Name of the Bidders/Firm / Company	
2	Constitution	
3	Date of Establishment/Incorporation	
4	Address	
	Registered Office Corporate Office	
5	Telephone No	
	FAX No	
	E-mail Address	
	Website	
6	Sales Turnover from IT related business. 2007-2008	
	2008-2009	
	2009-2010	
7	Domestic Customer Base (Number of Clients where Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services is implemented in India)	
8	Service Net Work (Number of Service Centers in)	
	North India	
	South India	
	East India	
	West India Central India	



Sl. No	Particulars	
<b>B.</b>	<b>Manufacturer's Profile</b>	
1	Name of the Manufacturing Company	
2	Constitution of the Manufacturing Company	
3	Date of Establishment/Incorporation of the Manufacturing Company	
4	Address of the Manufacturing Company Registered Office Corporate Office	
5	Telephone No FAX No E-mail Address Website	
6	Nature of Relationship of your company with the Manufacturing Company. Subsidiary of the Manufacturing Company/Division of Manufacturing Company/Sole Distributor/Non Exclusive Distributor/Agent/Others Please Specify	
7	Experience of the Manufacturing Company in Implementation of Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services	

Signature of the Authorised Signatory with date & seal



**ANNEXURE - D**

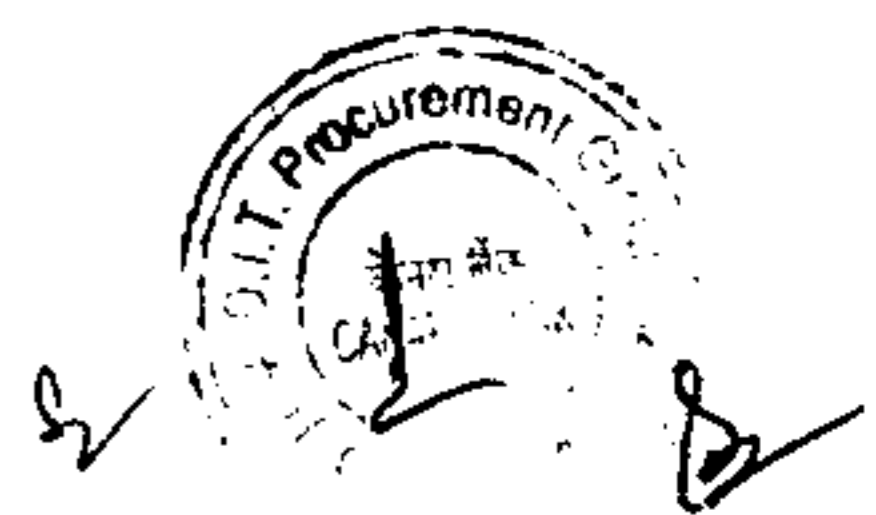
[Note: This details should be on the letter head of Bidder and should be signed by a an Authorised Signatory with Name and Seal of the Company]

**Track Record of Past Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services Solution**

Name of the Bidder \_\_\_\_\_

Sl. No.	Name of the Client	Implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services		Contact Person, Name, Tele No, FAX No & Address
		Description of the services implemented	Year of Implementation	
1				
2				
3				
4				

**Signature of the Authorised Signatory with date & seal**



**ANNEXURE - E**

[Note: This details should be on the letter head of Bidder and should be signed by a an Authorised Signatory with Name and Seal of the Company]

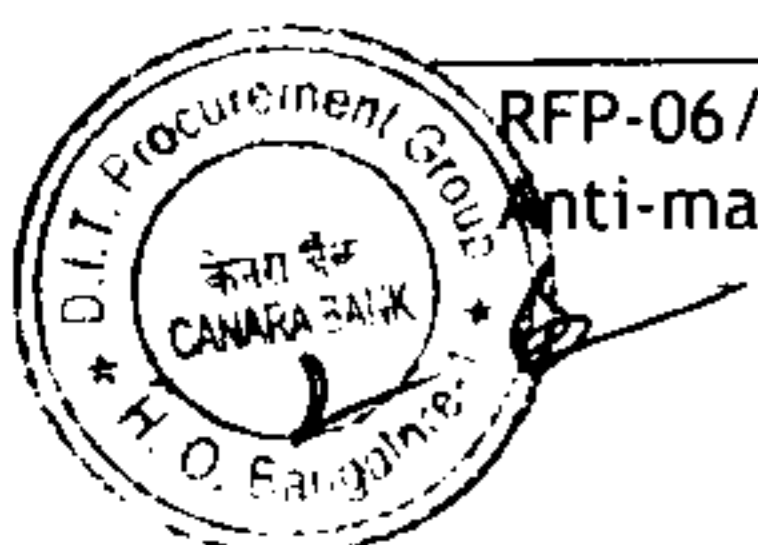
**Technical Compliance Statement**

Declaration

We hereby undertake to agree to abide by all the Instructions, Terms & Conditions including the Scope of Work stipulated in the RFP/tender document for smooth Implementation Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in Bank.

We certify that the systems / services offered by us for tender conform to the specifications stipulated in the tender form.

Signature of the Authorised Signatory with date & seal



**ANNEXURE - F**

[Note: This details should be on the letter head of Bidder and should be signed by a an Authorised Signatory with Name and Seal of the Company]

**Authorization letter format**

Date:

The Deputy General Manager,  
Canara Bank  
Asset Procurement & Management Group,  
DIT-Wing  
Naveen Complex, 14 M G Road,  
Bangalore - 560 001  
Karnataka

Dear Sir,

SUB: Authorization Letter for attending the Bid Opening

REF: Your RFP No. \_\_\_\_\_ Dated \_\_\_\_\_.

This has reference to your above RFP for implementation Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services in Canara Bank

Mr. Miss/Mrs. \_\_\_\_\_ is hereby authorized to attend the bid opening of the above RFP \_\_\_\_\_ DT: \_\_\_\_\_ on \_\_\_\_\_ on behalf of our organization.

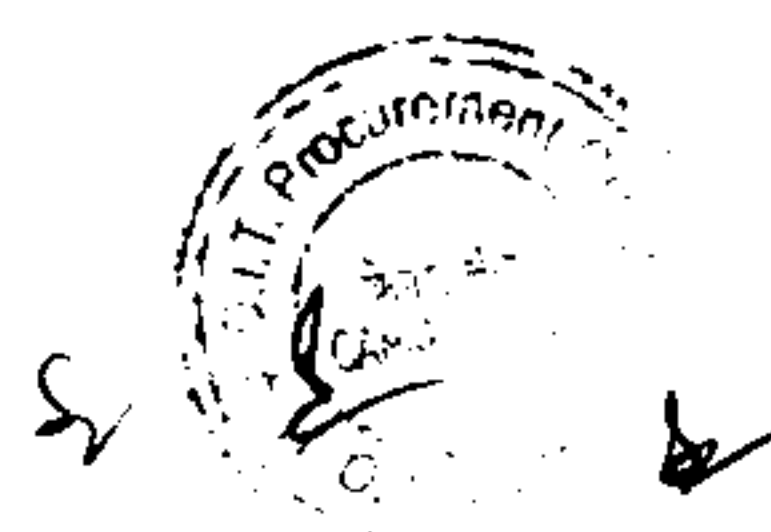
The specimen signature is attested below:

\_\_\_\_\_  
Specimen Signature of Representative

\_\_\_\_\_  
Signature of Attesting Authority  
With Name and Seal

\_\_\_\_\_  
Signature of Authorizing Authority

\_\_\_\_\_  
Name of Authorizing Authority



**ANNEXURE - G**

{Note: This Letter should be on the letterhead of the manufacturing concern and should be signed by a competent person of the manufacturer}

**Manufacturer's Authorization Form**

No. \_\_\_\_\_ dated \_\_\_\_\_

The General Manager,  
Canara Bank,  
Asset Procurement & Management Group,  
DIT-Wing,  
Naveen Complex, 14 M G Road,  
Bangalore-560 001  
Karnataka

Dear Sir,

Tender Reference No. \_\_\_\_\_

We \_\_\_\_\_ who are established and reputed manufacturers of \_\_\_\_\_ having factories at 1) \_\_\_\_\_ and 2) \_\_\_\_\_ do hereby authorize M/s \_\_\_\_\_ (Name and address of the Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the equipment and services offered against this invitation for tender offer by the above firm and will extend technical support for a period of 2 years from the date of purchase order and for any extended period that may be purchase order mutually agreed by both bank and the bidder.

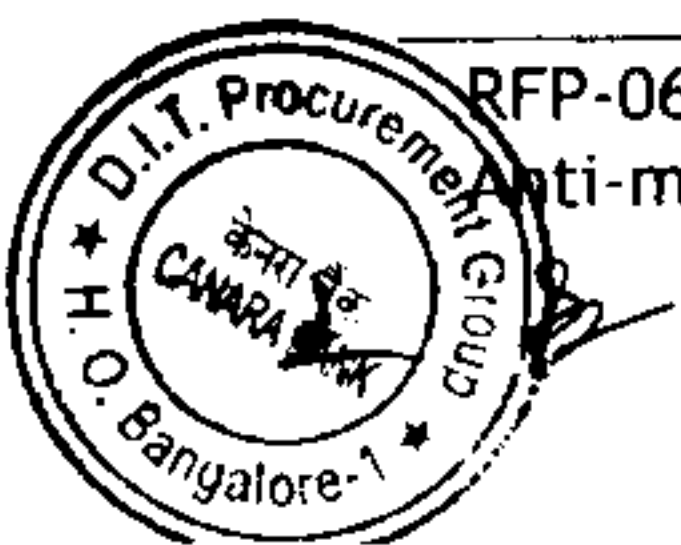
Yours faithfully

(Name)

For and on behalf of

M/s \_\_\_\_\_

(Name of Manufacturers)



**ANNEXURE - H**

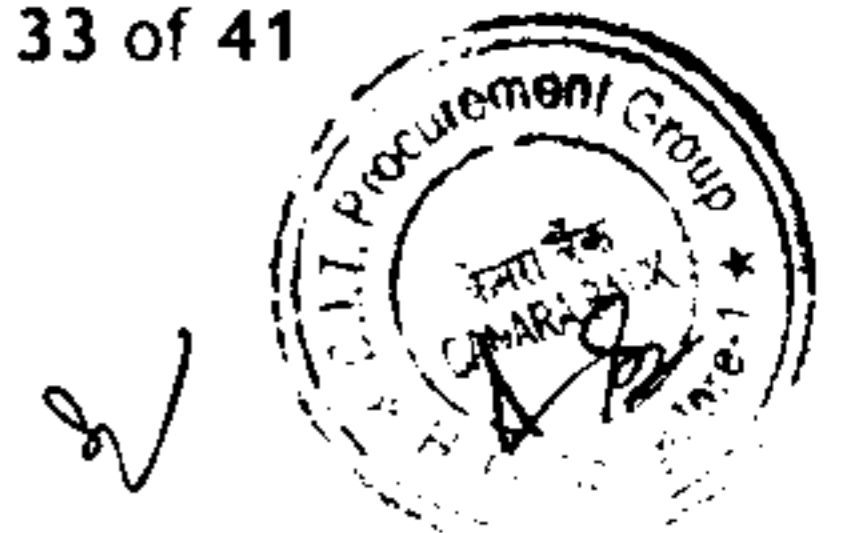
[Note: These details should be on the letter head of Bidder and each & every page should be signed by an Authorised Signatory with Name and Seal of the Company]

**Bill of Material and Price Schedule**

Note:

1. This Bill of Material must be attached in Technical Offer as well as Commercial Offer. The format will be identical for both Technical and Commercial Offers, **except that the Technical Offer should not contain any price information.** Technical offers without the Bill of Materials will be liable for rejection.
2. Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly.
3. The Commercial Bid will be evaluated based on the Total Cost of Ownership (TCO) and L1 Bidder will be determined.
4. The Bidder should indicate the individual taxes, and its applicable rate along with the estimated tax amounts to be paid by the Bank.
5. If any of the deliverable product, mainly, Hardware, software, Service/Support etc. has both VAT and Service Tax, the bidder has to indicate the Goods component with percentage of VAT and Service Component with service Tax involved. The Goods Component + Service Component should be limited to 100% of the Cost Price, For example, if Goods Component is 60% then, the Service Component cannot be more than 40%.

**Signature of the Authorised Signatory with date & seal**



**Bill of Material**

Sl No	Particulars	Description	Cost without tax amt per year ₹	Tax % of column (4)	Tax Amt of column (4)₹	Cost including tax per year ₹	No. of Years	Total cost including taxes ₹
1	2	3	4	5	6	7	8	9= 7 x 8
1	(a) Real-time online monitoring.	Anti-Phishing, Anti-Pharming, Anti-Malware					2	
	(b) For take-down of attacks with 200 attacks per year. **  This includes item Nos.(3.8) to (3.15) given in Scope of Work.	for all the sites listed in the scope of work.					2	
2	(a) Real-time online monitoring per year	Anti-Trojan, interception of underground activity related to Bank's associated credentials (A/c information of customers), Trojan email drop points					2	
	(b) Blocking of attacks with 200 attacks per year. **	Anti-Trojan, interception of underground activity related to Bank's associated credentials (A/c information of customers), Trojan email drop points					2	
3	Benchmarking of Bank's internet banking site and suggest controls required to minimize the impact from phishing attacks	This activity is to be done once in six months and a certificate to be given to that effect.						
<b>TOTAL COST OF OWNERSHIP (TCO)</b>								



*(Handwritten signature)*

\*\* This is taken for the purpose of arriving at L1. However, take down charges will be paid based on the unit rate arrived as above for the actual number of take downs.

**Note :**

1. Determination of L1 Price.

The Commercial Bid will be evaluated based on the Total Cost of Ownership (TCO) as per Bill of Material, i.e., Two year realtime online monitoring, take down/blocking of 200 attacks per year and Bench marking Bank's netbanking sites inclusive of taxes. Basing on the TCO, Ranking of the Bidders will be determined.

We understand that the above-mentioned figure is for price-comparison purpose only and for arriving the L1 Bidder.

We understand that Bank shall be placing Order to the Selected Bidder exclusive of taxes only and that all applicable Taxes like CST/VST/VAT/Service Tax will be paid at actual against production of invoice / bills.

We understand that Bank will pay VAT only for Good Component of Hardware/ Software and Service Tax for Service Component of Hardware/Software. We also understand that the Goods Component + Service Component should be limited to 100% of the Cost Price.

Date:

Signature of the Authorised Signatory with date & seal



Annexure - I

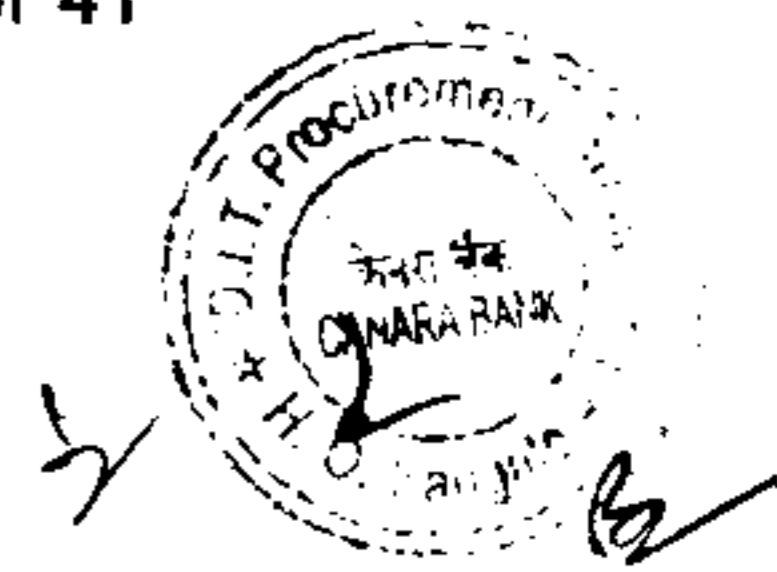
**Technical Specifications and Technical Evaluation Criteria**

SI No.	Parameter	Compliance Y/N	Remark/ Reference
1	The Bidder should have the ability to detect , monitor and shutdown all kind of incidents given below: <ul style="list-style-type: none"> <li>• Phishing</li> <li>• Pharming</li> <li>• Trojan</li> <li>• Malware</li> <li>• Brand abuse cases</li> <li>• Phishing/Trojan email drop points</li> <li>• Spoofing attacks</li> <li>• Monitoring of compromised servers</li> <li>• Domains registration</li> </ul>		
2	The Bidder should be capable of providing 24*7 support for all the activities listed above		
3	The Bidder should have DR set up to extend the support services in case of failure of main site		
4	The Bidder should be capable of communicating the incidents through various mode of communications such as email, Phone calls, SMS & dash boards		
5	The Bidder should be capable of providing regular updates about compromised accounts that are being stolen by various Trojans		
6	The bidder should have contacts /Tie ups with major Browser vendors, Internet Service Providers (ISPs) and other third parties to ensure faster closure of incidents. Should have tie ups with 1000+ ISPs in at least 50 countries		
7	The Bidder should have ability to track new domain registration, to detect any spoofed site being registered and take down the same on getting confirmation from bank		
8	The bidder should have the capability to communicate in the following languages: <ul style="list-style-type: none"> <li>• English</li> <li>• Hindi / Urdu</li> <li>• Arabic</li> <li>• Spanish</li> </ul>		



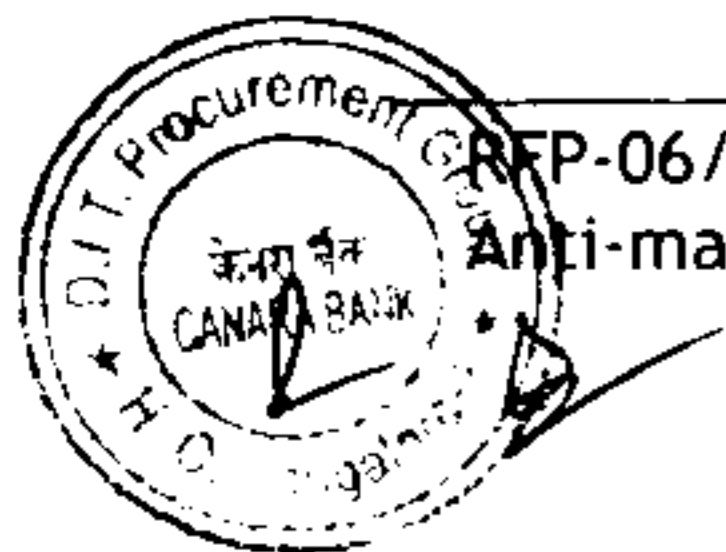


	<ul style="list-style-type: none"> <li>• Russian</li> <li>• German</li> <li>• Mandarin Chinese</li> <li>• Japanese</li> <li>• French</li> <li>• Portuguese</li> <li>• Indonesian</li> <li>• Bengali</li> </ul>		
<b>9</b>	<p>Detection capability should include monitoring Spam mails from various major services provides like Google, Yahoo, MSN, AOL etc.</p> <ul style="list-style-type: none"> <li>• Analysis of Internet Banking System web-server referrer logs other activities pertaining to phishing incidents</li> <li>• Monitoring of abuse mail box</li> </ul> <p>Monitoring of underground network through specialized services</p>		
<b>10</b>	<p>Forensics capability with the following functionalities wherever possible:</p> <ul style="list-style-type: none"> <li>• Comprehensive analysis of phishing mail, site and Trojan</li> <li>• Extracting critical data e.g. compromised accounts</li> <li>• Providing critical information to the customer as per the nature of the incident.</li> </ul> <p>Ability to provide data for investigation purposes</p>		
<b>11</b>	<p>Should be capable of extending Legal support in the form of communication with Cert-in / Cyber Crime on request from bank. Also extend technical support</p>		
<b>12</b>	<p>The Bidder should have the capability to integrate these services into Security operation Centre (SOC) on real time</p>		
<b>13</b>	<p>The Bidder should have capability to assist Bank in identifying customers affected by phishing attacks and recommend controls to minimize impact from phishing attacks</p>		
<b>14</b>	<p>The bidder should have capability to provide resolution of Phishing, Pharming, related incidents within 4 hours.</p>		
<b>15</b>	<p>The bidder should be providing their services across the globe with different brands</p>		



	heterogeneously to ensure maximum coverage of fraudulent activities across the globe.		
<b>16</b>	The bidder company / SOC should be ISO 27001 / BS 7799 certified		
<b>17</b>	The bidder Should have at least 5 skilled staff with CCN/CEH/CISA/CISSP/CISM/CVA Certification in their muster		
<b>18</b>	The bidder should provide Dashboard that should have all the following features: <ul style="list-style-type: none"> <li>• Regular update of incidents</li> <li>• Customized reports/ option to process ad-hoc queries</li> <li>• Help menu</li> <li>• Capacity to download extracted data</li> <li>• Availability of screen shots of all phishing related incidents</li> <li>• User access facility</li> <li>• Display of ongoing compliance status</li> </ul>		
<b>19</b>	The bidder should have capability/ willingness to share and disseminate information on fraud related activities with the members availing their services		

All the above points are compulsory and the bidders who satisfy the above requirements will be considered for next level of evaluation.

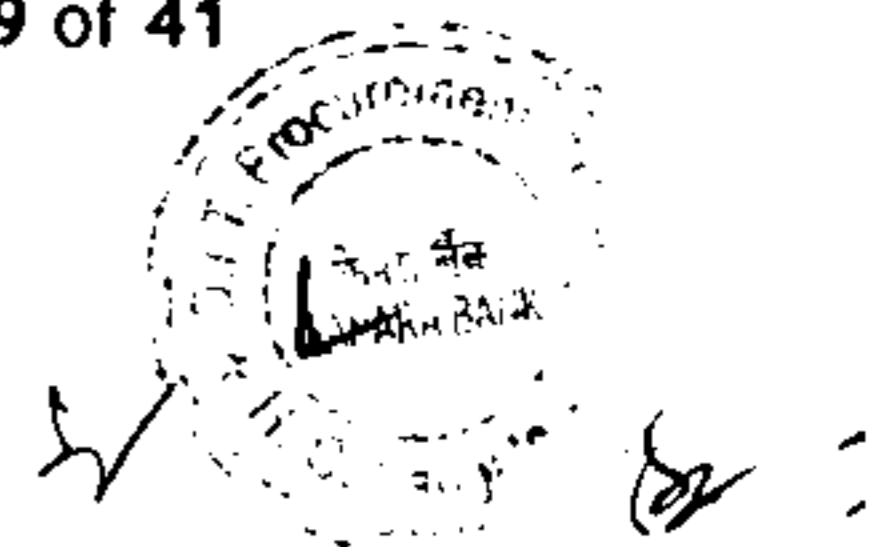




**Technical Evaluation Part II**

The table given below contains a score of 100. A bidder can participate in this table only if it complies with the previous one.

S.No	Parameters	Documents Required	Compliance	Score
1	No. of Tie ups with ISPs in more than 50 countries	Undertaking with the list of countries where there are tie ups	ISP support 50-75	2
			76-100	5
			>100 countries	10
2	No. of Direct tie ups with ISPs	Undertaking along with list of list of tie ups	1000 – 1500	2
			1501 – 2000	5
			>2000	10
3	No. of years of experience in Anti- phishing, Anti-Pharming, anti-Trojan, anti-malware services	Order copies / reference letters	1– 3 years	2
			>3 yrs upto 5 years	5
			>5 years	10
4	No. of Banking customers presently using the proposed services in India	Undertaking along with list of customers	2-5 customers	2
			6-10 customers	5
			>10 customers	10
5	No. of phishing, Pharming, Trojan incidents closed so far	Undertaking along with reports generated from database	50000-100000	2
			100001-150000	5
			>150000	10
6	No. of countries across which the shutdowns have been achieved	Undertaking and public datasheet / URL	50-100	2
			101-150	5
			>150	10
7	No. of spam mails scanned for phishing mail existence so far	Undertaking and public datasheet/URL	1-2 lacs	2
			>2 lac upto 5 lacs	5
			>5 lacs	10
8	Language support	Undertaking letter with list of languages	12 languages	2
			13 – 50 languages	5
			Above 50 languages	10
9	No. of CISA / CISM/ CISSP/ CIHE/ CVA/ CCSE security related certification holders in the organization	Profiles with copy of certification	Upto 5	5
			>5	10
10	ISO 27001 / BS 7799 certified	copy of the Certificate		10
Total (Maximum Score - 100)				



Annexure - J

**BANK GUARANTEE FORMAT FOR EARNEST MONEY DEPOSIT**

To

.....  
.....  
.....

WHEREAS \_\_\_\_\_(Name of Tenderer) (hereinafter called "the Tenderer" has submitted its tender dated \_\_\_\_\_ (Date) for the execution of (Name of Contract)\_\_\_\_\_ (hereinafter called "the Tender") in favour of \_\_\_\_\_ hereinafter called the "Employer";

KNOW ALL MEN by these presents that we, \_\_\_\_\_(name of the issuing Bank), a body corporate constituted under the \_\_\_\_\_having its Head Office at \_\_\_\_\_ amongst others a branch/office at \_\_\_\_\_ (hereinafter called "the Bank" are bound unto the employer for the sum of Rs \_\_\_\_\_(Rupees \_\_\_\_\_ only) for which payment well and truly to be made to the said Employer, the Bank binds itself, its successors and assigns by these presents;

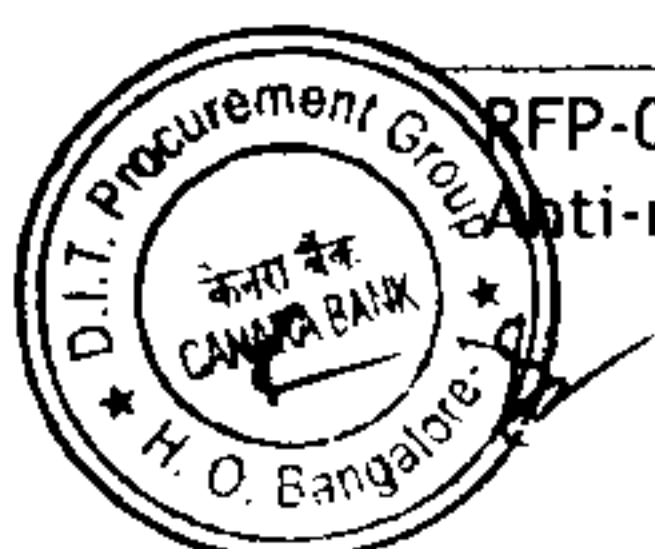
THE CONDITIONS of this obligation are:

- (a) If the Tenderer withdraws its Tender during the period of Tender validity specified in the Tender; or
- (b) If the Tenderer having been notified of the acceptance of his Tender by the Employer during the period of Tender validity;
  - (i) fails or refuses to execute the Agreement, if required; or
  - (ii) fails or refuses to furnish the performance security, in accordance with clause \_\_\_\_\_ of conditions of Contract.

We undertake to pay to the Employer up to the above amount upon receipt of his first written demand without the Employer having to substantiate his demand, provided that in his demand the Employer will note that the amount claimed by him is due to him owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

Notwithstanding anything contained herein

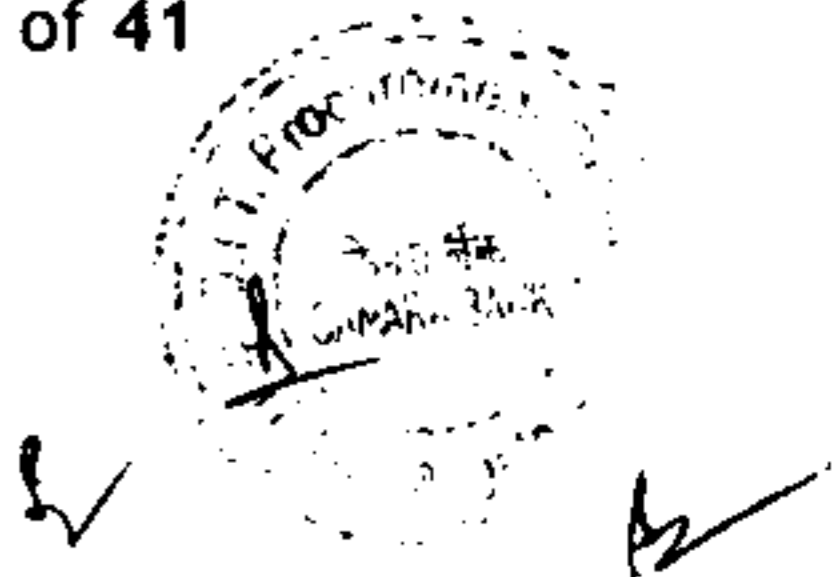
- i) Our liability under this Bank Guarantee shall not exceed Rs. \_\_\_\_\_ (Rupees \_\_\_\_\_ only)
- ii) This Bank Guarantee is valid up to \_\_\_\_\_ and



iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before \_\_\_\_\_ (mention period of guarantee as found under clause (ii) above plus claim period)

Dated \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_

SIGNATURE & SEAL OF THE BANK



1000