PUNJAB NATIONAL BANK

(Open Tender)
Request For Proposal (RFP) for Procurement of Network Anti-Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

Punjab National Bank
Information Technology Division
Head Office, 5 Sansad Marg,
New Delhi - 110 001
Tel: (011)- 23765468

DISCLAIMER

The information contained in this Request for Proposal Document (RFP Document) or subsequently provided to Bidder/s, whether verbally or in documentary form by or on behalf of the Punjab National Bank or any of their representatives, employees or advisors (collectively referred to as — Bank Representatives), is provided to Bidder(s) on the terms and conditions set out in this RFP Document and any other terms and conditions subject to which such information is provided. This document shall not be transferred, reproduced or otherwise used for purpose other than for which it is specifically issued.

This RFP Document is not an agreement and is not an offer or invitation by the Bank Representatives to any party other than the entities who are qualified to submit their Proposal (Bidders). The purpose of this RFP Document is to provide the Bidder with information to assist the formulation of their Proposal. This RFP Document does not purport to contain all the information each Bidder may require. This RFP Document may not be appropriate for all persons, and it is not possible for the Bank Representatives, their employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP Document.

The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process. The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder’s risk and may result in rejection of the Bid.

The Bank Representatives may in their absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP Document.

TABLE OF CONTENTS

GENERAL TENDER DETAILS

RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.		
1.	Date of commencement of Bidding Process.	08/07/2019
2.	Last date and time for sale of Bidding Documents	30/07/2019 upto 1600 Hrs
3.	Last date and time for receipt of queries from bidders for Clarifications	10/07/2019 upto 1700 Hrs
4.	Date of Pre-Bid Meeting	11/07/2019 at 1500 Hrs
5.	Last date and time for Hash submission	30/07/2019 upto 1600 Hrs
6.	Last date and time for online bid submission/Bid Re-Encryption	From 30/07/2019 1701Hrs to 31/07/2019 1400 Hrs
7.	Last date and Time for submission of technical supporting document (Hard Copy)	From 30/07/2019 1701 Hrs to 31/07/2019 1400 Hrs
8.	Date and Time of Technical Bid Opening	31/07/2019 at 1600 Hrs
9.	Place of Submission of Bids	The Asstt. General Manager Punjab National Bank, IT Procurement Department, I.T. Division, HO: 5 Sansad Marg, New Delhi 110 001
10.	Place of opening of Bid	Punjab National Bank, Information Technology Division, 2nd floor, HO, 5 Sansad Marg, New Delhi – 110 001.
11	Address for communication	As above Tel:- (011) 23765468
12.	Cost of RFP	**Rs.5000/-+ 18 % GST*(**Non-refundable) should be submitted **online only** in favour of Punjab National Bank before last date of bid submission in the following account: IFSC Code : PUNB0399900 Bank & Branch : Punjab National Bank, Sansad Marg, New Delhi -110 001 Account No**. 0153002200175673** (16 digits) Imprest account – HO IT Division *MSME bidder is exempted from payment of cost of RFP if bidder can furnish requisite proof subject to the satisfaction of Bank.
13.	Earnest Money Deposit	**Rs.20.00 Lac***should be submitted online before last date of bid submission or in the form of Bank Guarantee (BG) in favour of Punjab National Bank, IT Division payable at New Delhi. BG should be valid up to 6 months from the last date of submission. IFSC Code : PUNB0015300 Bank &Branch : Punjab National Bank, Sansad Marg, New Delhi -110 001 Account No. **0153002100572949** (16 digits) Imprest account – HO IT Division *MSME bidder is exempted from payment of Earnest Money Deposit if bidder can furnish requisite proof subject to the satisfaction of Bank.

14.	Contact to Bidders	Interested Bidders are requested to send the email to **swapnika.sonker@pnb.co.in, rohitraina@pnb.co.in,** containing following information, so that in case of any clarification, the same may be issued to them: (a)Name of Bidder, (b)Contact person, (c)Mailing address with Pin Code,(d)Telephone No., Fax No., Mobile No.(e) e-mail etc.

NOTE

1. All the interested Bidders, who have not registered earlier with e-procurement site(https://etender.pnbnet.in), would have to register with our e-procurement site. Bidders to ensure to get themselves registered timely, at least Two working days before the Hash submission date, to avoid last moment issues.
2. Bidders are advised to go through Bidders Manual available on https://etender.pnbnet.in for registration and submission of tenders. If approval of registration is pending at Bank's end, Bidders should immediately contact Bank's Helpdesk on telephone No. 011-23765468 or email us at eprocurement@pnb.co.in
3. Bidders are required to strictly submit their bids in electronic form using the e-procurement system at https://etender.pnbnet.in by using their digital certificates of class II and above (both encryption and signing). Bidders are advised to keep digital certificates(or tokens) ready at time of submission of bid. Use of Digital Certificate is mandatory for participation in e-tendering process. Bidders should ensure that Digital token has not expired or corrupted at the time of e-tendering process.
4. Bidders are advised to go through Bidders Manual for Browser settings and Java settings required for participation in the bid. Follow each & every step mentioned in Bidder Manual. If bidder still faces any problem, he/she should immediately contact Bank Helpdesk on telephone No. 011-23765468 or email us at eprocurement@pnb.co.in.
5. Bids received after closing of the bid in the e-procurement system will be auto-rejected by the system. Please note that **HASH SUBMISSION and BID RE-ENCRYPTION** is a mandatory activity, failing which Bank will not accept the hardcopy of Technical bid.
6. The indicative commercial bids to be submitted online only.
7. Bidders should submit bids well before time rather than waiting for last moment to avoid any technical glitches or networking issues etc. at their end.
8. If bidder is shortlisted to participate in Reverse Auction (RA), Demo for Reverse Auction will be conducted a day before RA, if bidder requests for the same. Further, Demo for Reverse Auction will only be provided to bidders who have accepted the Base price (i.e. Terms & Conditions of the reverse auction).
9. If bidder is participating in the Reverse Auction, it is advised that Bidders place their bids well before time rather than waiting for auction end time to avoid any last minute glitches (or any network issues or internet response issues etc.) occurring at Bidder's end. Bidders may keep refreshing auction page to ensure that they are connected to server (via internet).
10. Bidders are requested to use a reliable internet connection (data cable/ broad band) to safeguard themselves. Bank is not responsible for telephone line glitch, internet response issues, hardware hangs etc., at bidder's end.
11. If Bidders have any queries, they may call us at Helpdesk Telephone No 011-23765468 from 10.00 am to 05.00 pm (except Sundays and Bank holidays).

1. INTRODUCTION:

Punjab National Bank (PNB) has taken many IT initiatives. Bank has Computerized 100% of its branches and has implemented a Centralized Banking Appliance (CBS) with Data Centre at New Delhi and Disaster Recovery Site at Mumbai. The centralized Banking Appliance covers all the 7000 plus SOLs (Service Outlets), which are connected to the Data Centre and DRS through an Enterprise Wide Network which is a two tier meshed architecture. The mode of connectivity to the branches/offices is a combination of Leased Lines, ISDN Lines, MPLS, VSATs, Radio Links and other forms of connectivity, which may emerge in the near future.

Bank has also implemented Security Operation Centre (SOC) and integrated the servers / devices for log analysis and monitoring of servers / devices installed across the Bank network. Bank has implemented Enterprise Data Ware House Project to provide better access to information, to foster better and more informed decision-making, besides providing statutory reporting and MIS for the Bank.

The Enterprise Wide Network is maintained by Bank's Network Integrator and the security measures are already enforced at various levels (Application Security, Network Security, Database Security, OS Security, Access Controls, Physical Security etc.). All these security measures are in place in congruence with the Bank's Information Security Policy, Business Continuity & Disaster Recovery Plans & various other regulatory compliances.

2. PURPOSE OF THE PROJECT:

An advanced persistent threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization. The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible. To prevent the above mentioned type of attack, the Bank intends to purchase Anti-APT solution to monitor the threat of both internal and external traffic.

The deception solution is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage. The solution works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials. Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal. Bank intends to use this technology which can detect, analyze, and defend against attacks including zero-day and advanced attacks, often in real time.

The purpose of this RFP is to select a vendor for supply, implementation and maintenance of an Anti-APT Solution for Bank's network and Deception solution with the objective of securing Bank's data thereby augmenting Bank's existing Security architecture.

Punjab National Bank invites bids (Technical bid and Commercial bid) from eligible bidders for as per requirements mentioned in the RFP. This invitation of Bids is open to all Original Equipment Manufacturers (OEMs) having presence in India or their Authorized Representative in India, provided bidders fulfill the minimum qualification criteria as mentioned in bid document (Annexure-III).

Please note that any deviations mentioned in the bid will not be considered and evaluated by the Bank. Bank reserve the right to reject the bid, if bid is not submitted in proper format as per RFP.

3. SCOPE OF WORK:

The Scope of Work includes the following components :-

For Network Anti-APT Solution

3.1. The Bidder shall be responsible for supply, implementation and maintenance of Network Anti-APT Solution at Bank's Data Centre & Disaster Recovery Centre.

3.2. The proposed Anti-APT solution should be seamlessly integrated with the Bank's SIEM solution, Firewall, Proxy to generate alerts for any Anti - APT violations and with the existing Endpoint APT Solution or any other existing or future solution, as required by the Bank.

3.3. The complete implementation of the solution is to be done by the OEM. Bidder has to arrange for OEM's resources and the bidder will be responsible for all co-ordination with the OEM and for completion of the implementation, within the timelines. At the end of the implementation, the bidder has to arrange for a Certificate from the OEM, certifying that the implementation has been done by OEM's Resources and the deployed solution meets all the technical/functional specification of the solution as specified in Annexure-XII of this RFP.

3.4. The Bidder is required to Supply & install all the required Hardware and Software (OS, Database& Application) with required licenses (Perpetual) and also Provide, cables, connectors etc. required to commission the ATP Solution infrastructure. Bank will only provide the required Physical Infrastructure (power, cooling, rack space etc.). Cost of all the peripherals hardware/accessories which are to be provided by the bidder should be included in cost of hardware in the indicative commercial bid.

3.5. The Solutionshould be sized for 100Mbps performance throughput and the solution (with each of its components) should be configured in High Availability (HA) mode both at DC& DR. The bidder should size for adequate hardware and related software and the proposed solution should have the functionality to scale both horizontally and vertically.

3.6. The bidder should

a. Provide incident management workflow and process as per best practices with respected to solution provided.
b. Provide a Centralized Management Console with customizable dashboard and role-based admin.
c. Provide online portal access covering the APT threats and Zero day attacks and Alert the designated PNB officials when an APT attack or a Zero day attack is detected in APT solution provided. This service should be available round the clock.
d. Provide Monthly / quarterly Advanced Malware reporting on incidents across the industry or geo-specific reports.
e. Proactive immediate notifications of serious system health issues for the deployed APT solutions.
f. Conduct System/Solution health check-up twice a year and provide report to the Bank.

g. Monitor events from anti-APT and suggest & take appropriate action on an on-going basis.
h. Develop and improve the policies configured on an on-going basis to reduce the occurrence of false positives.

3.7. The bidder shall develop a Project Management Plan which shall address the following Service(s) processes:

- Document Control
- Change Management
- Inspection and Testing

3.8. The Bidder shall provide the technical design document including
a. Product details.
b. Administrative Guide
c. Troubleshooting Guide Basic and Advanced
d. System Performance benchmarks (data sheet for the hardware used, etc.)
e. Architecture (diagram).

3.9. If Load Balancing is required for the implementation of the Solution, the bidder has to arrange for the same, without any extra cost to the Bank. Bank will not provide any hardware/software for load balancing.

3.10. The Vendor should maintain Uptime of **99.95%** of the Solution quarterly both at DC & DRS during contract period. The Dashboard of the solution should show daily Uptime of the solution.

3.11. If Bank requires any customization in the solution, during the entire period of contract, the bidder will have to implement the same without any extra cost to the bank.

3.12. **End of Sales / End of support:** The Vendor has to ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales on the date of such supply or end of support for at least 5 year from the date of issue of purchase order. In the event if any equipment supplied by the vendor reaches end of support, within the contract period from the date of supply, the vendor has to replace the equipment at no additional cost to the Bank.

3.13. **Training-** Vendor is required to impart training to the identified bank personnel/ SOC team on the product architecture, functionality and solution design before the start of implementation of the solution. In addition to that, mandatory training of atleast One week is to be provided to Bank staff (10 officials) twice in the first year of Contract (at a minimum gap of 6 months), with complete knowledge transfer for handling the application or regarding any new feature/update etc, at no extra cost to the Bank. The training shall cover functional, operational and reporting aspects of the entire APT solution along with product architecture.

3.14. **Onsite Technical Support (OTS)-** Minimum two L2 resources must be deployed by the bidder from 8:00 AM to 8:00 PM, during implementation period, in addition to the OEM's resources. One L2 resource(OEM certified Resource provided by the OEM itself) must be deployed at DC at normal shift (10:00 am to 6:00 pm) for One Year post Implementation i.e. one year from sign-off, without any extra cost to the Bank. The L2 resources deployed should have requisite knowledge and experience of atleast 3 years of the deployed solution, required for management and monitoring of the overall operations of ATP Solution. A certificate from the OEM is required in this regard,

certifying that the deployed resource has atleast 3 yrs of experience of the APT solution. Bank may carry out security verification of the deployed resources.

After One Year of implementation of complete Solution, Bank may avail additional OTS, at any time during the remaining contract period of 4 years. Separate commercials have been called for the Onsite Technical Support and it is the sole discretion of the Bank to avail its services or the duration of the OTS. Separate Purchase Order will be issued for the OTS (after 1 year of implementation) specifying the duration of the support and the no. of engineers required. Bank is not bound to place any minimum order for additional OTS. This option will be availed as and when required by the Bank.

The non-availability of resource for any of the support resources, should be compensated with a resource having similar skill set for the period of non availability. The penalty for non-availability of the resource would be applicable as mentioned in clause 14.3 of Annexure-I. The Bank reserves the right to interview the resources that would be deployed at the Bank DC Location for Onsite Technical Support.

3.15 **Information Security and Audit**- Bidder will provide an undertaking to comply with all the present and future provisions of the Information Security Policy/NPCI Guidelines/Guidelines of RBI, Respective Govt. Agencies and the Bank and provide such regulatory requirements at no additional cost to bank during the warranty and ATS/AMC period. The Solution may be audited by RBI/any other Regulatory Authority and any observation pointed out by these bodies have to be complied by the vendor within the timelines stipulated by the regulatory agencies, without any additional cost to the Bank. The offered solution shall be subjected to Bank's audit (including VAPT, EAPT and functional audit of the solution) through off-site and on-site scrutiny at any time during the contract period. The auditors may be internal/ external. The vendor should provide solution and implementation for all the audit points raised by bank's internal/external team during the contract period, within the stipulated timelines, without any extra cost.

For Deception Solution

3.16. The proposed Deception solution should be able to address the following key areas but not limited:

1. Effectively create a replica copy of the Bank's existing infra with real operation systems
2. Hacking incentive of the proposed decoy ecosystem should be as equivalent to present exposed incentive of the Bank
3. The intended solution must safeguard the Bank against a target attack, and also act as a layer of defense for attacks based on new-vulnerabilities, Anti phishing attacks, data theft and zero day attacks etc.
4. Should provide real time Alerts or email

3.17. The Bidder shall be responsible for supply, implementation and maintenance of Deception Solution on the Bank's existing network (DC, DR, DMZ, endpoints & branches) as deemed by the Bank, without affecting the existing environment and traffic.

3.18. The complete implementation of the solution is to be done by the OEM. Bidder has to arrange for OEM's resources and the bidder will be responsible for all co-ordination with the OEM and for completion of the implementation, within the timelines. At the end of the implementation, the bidder has to arrange for a Certificate from the OEM, certifying that the implementation has been done by OEM's Resources and the deployed solution meets all the technical/functional specification of the solution as specified in Annexure-XII of this RFP.

3.19. The bidder should create decoy versions of real servers, desktops, files, users accounts, applications like SWIFT/NEFT/RTGS/Core banking etc. and using them as traps. These traps or decoys should be placed at bank's DC & DR network.

3.20. The decoys should be scientifically placed in multiple subnets, so the hackers will encounter them in the process of trying to find valuable information. When the hackers try to access the decoys, a silent alert is raised and full forensics about the attack is collected.

3.21. Decoys should be customized and tailored to the bank's environment by mimicking real servers , and applications making them blend in completely

3.22. The solution should not rely on signature or behavior patterns, thereby providing effective approach in detecting advanced attacks including malware-less attacks that can circumvent existing preventive controls.

3.23. The proposed Deception solution should be seamlessly integrated with the Bank's Active Directory and with SIEM solutions and should provide monitoring and network visibility as well as early detection of attacks while keeping false positives to almost nil as well as any other security solutions so as to take intended action to block or take action against the affected assets and any other existing or future solution, as required by the Bank.

3.24. The Bidder is required to Supply all the required Hardware and Software (OS, Database & Application) with required licenses (perpetual) and also Provide, cables, connectors etc. required to commission the Deception Solution infrastructure. Bank will only provide the required Physical Infrastructure (power, cooling, rack space etc.). Cost of all the peripherals hardware/accessories which are to be provided by the bidder should be included in cost of hardware in the indicative commercial bid.

3.25. The Solution should be sized for approx. 150 VLANs at DC & 100 VLANs at DRS and total 1200 servers. Bank has approx. 20000 endpoints across 7000 branches. The solution (with each of its components) should be configured in High Availability (HA) mode both at DC& DR. The bidder should size for adequate hardware and related software and the proposed solution should have the functionality to scale both horizontally and vertically.

3.26. The bidder should Provide a Centralized Management Console with customizable dashboard and role-based admin.

3.27. Bidder should conduct System/Solution health check-up twice a year and provide report to the Bank.

3.28. The bidder shall develop a Project Management Plan which shall address the following Service(s) processes:

- Document Control
- Change Management
- Inspection and Testing

3.29. The Bidder shall provide the technical design document including

a. Product details.

b. Administrative Guide

c. Troubleshooting Guide Basic and Advanced

d. System Performance benchmarks (data sheet for the hardware used, etc.)

e. Architecture (diagram).

3.30. If Load Balancing is required for the implementation of the Solution, the bidder has to arrange for the same, without any extra cost to the Bank. Bank will not provide any hardware/software for load balancing.

3.31. The Vendor should maintain Uptime of **99.95%** of the Solution, quarterly both at DC & DRS during contract period. The Dashboard of the solution should show daily Uptime of the solution.

3.32. If Bank requires any customization in the solution, during the entire period of contract, the bidder will have to implement the same without any extra cost to the bank.

3.33. **End of Sales / End of support:** The Vendor has to ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales on the date of such supply or end of support for at least 5 year from the date of issue of purchase order. In the event if any equipment supplied by the vendor reaches end of support, within the contract period from the date of supply, the vendor has to replace the equipment at no additional cost to the Bank.

3.34. **Training-** Vendor is required to impart training to the identified bank personnel/ SOC team on the product architecture, functionality and solution design before the start of implementation of the solution. In addition to that, mandatory training of atleast One week is to be provided to Bank staff (10 officials) twice in the first year of Contract (at a minimum gap of 6 months), with complete knowledge transfer for handling the application or regarding any new feature/update etc, at no extra cost to the Bank. The training shall cover functional, operational and reporting aspects of the entire Deception solution along with product architecture.

3.35. **Onsite Technical Support (OTS)-** Minimum two L2 resources must be deployed by the bidder from 8:00 AM to 8:00 PM, during implementation period, in addition to the OEM's resources. One L2 resource(OEM certified Resource provided by the OEM itself) must be deployed at DC at normal shift (10:00 am to 6:00 pm) for One Year post Implementation i.e. one year from sign-off, without any extra cost to the Bank. The L2 resources deployed should have requisite knowledge and experience of atleast 3 years of the deployed solution, required for management and monitoring of the overall operations of Deception Solution. A certificate from the OEM is required in this regard, certifying that the deployed resource has atleast 3 yrs of experience of the Deception solution. Bank may carry out security verification of the deployed resources.

After One Year of implementation of complete Solution, Bank may avail additional OTS, at any time during the remaining contract period of 4 years. Separate commercials have been called for the Onsite Technical Support and it is the sole discretion of the Bank to avail its services or the duration of the OTS. Separate Purchase Order will be issued for the OTS (after 1 year of implementation) specifying the duration of the support and the no. of engineers required. Bank is not bound to place any minimum order for additional OTS. This option will be availed as and when required by the Bank.

The non-availability of resource for any of the support resources, should be compensated with a resource having similar skill set for the period of non availability. The penalty for non-availability of the resource would be applicable as mentioned in clause 14.3 of

Annexure-I. The Bank reserves the right to interview the resources that would be deployed at the Bank DC Location for Onsite Technical Support.

3.36 **Information Security and Audit**- Bidder will provide an undertaking to comply with all the present and future provisions of the Information Security Policy/NPCI Guidelines/Guidelines of RBI, Respective Govt. Agencies and the Bank and provide such regulatory requirements at no additional cost to bank during the warranty and ATS/AMC period. The Solution may be audited by RBI/any other Regulatory Authority and any observation pointed out by these bodies have to be complied by the vendor within the timelines stipulated by the regulatory agencies, without any additional cost to the Bank. The offered solution shall be subjected to Bank's audit (including VAPT, EAPT and functional audit of the solution) through off-site and on-site scrutiny at any time during the contract period. The auditors may be internal/ external. The vendor should provide solution and implementation for all the audit points raised by bank's internal/external team during the contract period, within the stipulated timelines, without any extra cost.

Other conditions:

a. The vendor will provide services for implementation / rolling-out /support / maintenance of proposed Solutions for a minimum period of 5 years (3 years warranty + 2 years AMC/ATS) from installation date with option of further extension of contract for another two terms of 1 year each, at the same rate & same terms & conditions, provided services of the bidder is satisfactory and at Bank's sole discretion. Bank reserves right to cancel the contract at any time in case system fails to meet any of the requirements as mentioned in the RFP.

b. No right to employment in the Bank shall accrue or arise, at any point of time under this project.

c. A detailed agreement will be done with the vendor specifying roles and responsibilities.

d. Obtaining of the Road permits or any other document for delivery of the material till Bank's premises will be the sole responsibility of the vendor. The vendor shall arrange road permit for locations applicable at no extra cost to the Bank. However, Bank will sign the necessary forms as purchaser, as per the requirements.

INSTRUCTION TO BIDDERS

1. POWER OF ATTORNEY/ AUTHORIZATION LETTER OR RESOLUTION COPY

In case of company, Board Resolution in favour of Authorized Person and Power of Attorney/Authorization letter (from authorized person executed on stamp paper of appropriate value), in case the authorized person delegates authority to another person of the company to sign the Bid documents, is to be submitted with bid documents.

2. COST OF BIDDING

The Bidder shall bear all the costs associated with the preparation and submission of their bid and Punjab National Bank, hereinafter referred to as “Purchaser” or "Bank”, will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

3. BIDDING DOCUMENT

The Bidder is expected to examine all instructions, forms, terms and conditions in the Bidding Documents. Failure to furnish all information required by the Bidding Documents or submission of a bid not substantially responsive to the Bidding Documents in every respect will be at the Bidders’ risk and may result in the rejection of its bid without any further reference to the bidder. Bidder should submit the bid strictly as per RFP failing which bid will be treated as non-responsive and will be liable for rejection.

4. LANGUAGE OF BIDS

The bids prepared by the bidder and all correspondence and document relating to the bids exchanged by the bidder and PNB, shall be written in English.

5. AUTHENTICATION OF ERASURES/ OVERWRITING ETC.

Any inter-lineation, erasures or overwriting shall not be valid and it will lead to rejection of bid without quoting any reason.

6. AMENDMENT OF BIDDING DOCUMENTS

At any time prior to the last Date and Time for submission of bids, the Bank may, for any reason, modify the Bidding Documents through amendments at the sole discretion of the Bank. All amendments shall be uploaded on the Bank’s websites (and https://etender.pnbnet.in) and will be binding on all those who are interested in bidding in order to provide prospective Bidders a reasonable time to take the amendment if any, into account in preparing their bid, the Bank may, at its discretion, extend the deadline for submission of bids. Bidders are required to go through the any subsequent amendment/Corrigendum/clarifications meticulously and submit their queries, if any, at least 2 working days before the hash submission date to avoid any last minute issues.

7. VALIDITY OF BID DOCUMENT

Bid shall remain valid for 6 months from last date of submission of bid prescribed by PNB. A bid valid for shorter period shall be rejected by the purchaser as non-responsive.

8. LATE BID

Any bid received by the Bank after the deadline for submission of bid will be rejected.

9. BID CURRENCY

Prices shall be expressed in the Indian Rupees only.

10. BID EARNEST MONEY

Bidder has to submit the Bid Earnest Money (EMD) of **Rs. 20.00 lacs**, which may be submitted in the form of online deposit or Bank Guarantee (BG) favoring PUNJAB NATIONAL BANK, IT DIVISION New Delhi and filling all the details as per specified Performa at **Annexure-XIV**. The Bank Guarantee should be issued by any Public Sector Bank or scheduled Commercial Bank other than Punjab National Bank. The BG should have a validity of 6 Months from the last date of submission of bid. Bidder shall be responsible to get the same extended for a further period of 6 months, if required by the Bank. The BG should be submitted at the time of bid submission. MSME bidder is exempted from payment of EMD if bidder can furnish requisite proof subject to the satisfaction of Bank.

In case of unsuccessful bidder, EMD will be returned either on completion of tender process or within one month of disqualification of the bidder, as per Bank's discretion. No interest will be payable on EMD amount. The EMD will be returned to the successful bidder upon submission of Performance Bank Guarantee and no interest will be payable on EMD amount.

Details for online payment:
IFSC Code: PUNB0015300
Bank& Branch: Punjab National Bank, Sansad Marg, New Delhi -110001
Account No. 0153002100572949 (16 digits) Imprest account – HO IT Division

(Proof of the transaction (printout) to be submitted along with the bid documents).

11. BIDDING PROCESS (TWO STAGES)

For the purpose of the present job, a two stage bidding process will be followed. The response to the present tender will be submitted in two parts:

- Technical bid
- Commercial bid

The bidders will have to submit the technical bid in Banks e-procurement system as well as in hard copy and commercial bids in only online form through Bank's e-procurement system. All documents/letters, addressed to the Bank, should be submitted in Original. (No Photocopies will be acceptable).

a) TECHNICAL BID

The Technical bid must be submitted in hard bound file in a sealed envelope superscribing "**Technical Bid response against RFP FOR Procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.**"& also online. Unsealed envelops will not be accepted. TECHNICAL BID will contain all the supporting documents regarding eligibility criteria, scope of work, Technical aspects, Compliance statement and Terms & Conditions etc. mentioned in the RFP, and **NOT contain any pricing or commercial information at all**. Technical bid documents with any commercial information will be rejected.

In the first stage, only TECHNICAL BIDs will be opened and evaluated. Bids of only those bidders would be evaluated further on Technical parameters who comply with all the eligibility criteria's. Only those bidders confirming compliance to all the terms &conditions of RFP document and Technical functionalities shall be short-listed for commercial stage.

b) COMMERCIAL BID

In the second stage, the COMMERCIAL BID of only those bidders will be opened, who will comply will all the eligibility criteria's and will confirm compliance to all the terms & conditions of RFP document and Technical functionalities in the Technical Evaluation Stage. **(Annexure-XII)**

12. Pre-Bid Meeting & Pre-Bid Queries.

Bidders/OEMs are required to submit pre-bid queries, within the stipulated timelines as given in the General Tender Details, through mail (In excel format only). Bidders are also required to bring hard copy of the same queries on their letter head, duly signed and stamped by their authorized signatory. **Queries not submitted in hard copy will not be responded.**

Sr.No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks

The queries submitted before pre-bid meeting and submitted in hard copy as mentioned above, will only be discussed in the pre-Bid meeting and their subsequent responses will be uploaded onto Bank's websites.

Only two persons per bidder/OEM will be allowed to attend the Pre-Bid meeting provided they have authorization letter from competent authority to attend the pre-bid meeting from their company. Bidders/OEM attending the pre-bid are also required to submit a copy of their I-card issued by their company.

No person shall be allowed to attend the Pre-Bid meeting without Proper Authorization letter from their Company and without their Official ID Cards issued by their company.(Any other ID proof such as PAN, DL or Aadhar card will not be accepted)

Bidders are required to go through the RFP and any subsequent Corrigendum's/clarifications meticulously and submit their queries timely to avoid any last minute issues.

13. SUBMISSION OF BID

Bidders are required to strictly submit their bids in electronic form using the e-procurement system at https://etender.pnbnet.in by using their digital certificates of **Class II** and above (both encryption and signing). All the interested bidders should register themselves in the e procurement system https://etender.pnbnet.in for submitting the bids online, if they have not done earlier. The RFP document and further corrigendum, if any can also be downloaded from Bank's websiteswww.pnbindia.in & https://etender.pnbnet.in. Bids received after closing of the bid in the e-procurement system are summarily rejected without any reason.

The commercial bid should be submitted online only.

All the Annexures and bid documents are to be uploaded in pdf format during the online bid submission and the same along with technical supporting documents should be submitted manually before the final date & time of bid submission at the following address.

The Asstt. General Manager
Punjab National Bank,
IT Procurement Department,
I.T. Division, HO: 5 Sansad Marg,
New Delhi 110 001

The hard copy of the technical bid to be submitted should contain all the required annexures in original. Bidder to ensure submission of bid strictly as per the requirement of the RFP. **Kindly do not submit any extra documents/certificate which are not required.** At the time of physical submission of bid, bidder has to show acknowledgement e-mail received after completion of the bid submission in proof of having submitted the bid online.

14. DEADLINE FOR SUBMISSION OF BID

Bids must be submitted not later than the specified date and time mentioned in the Bid Document. If the specified date of submission of bids being declared a holiday for the Purchaser, the bids will be received up to the specified time in the next working day. The Purchaser may, at its discretion, extend this deadline for submission of bids by amending the bid documents, in which case all rights and obligations of the Purchaser and bidders,

previously subject to the deadline, will thereafter be subject to the deadline extended. All the correspondence should be addressed to Bank at the following address.

The Asstt. General Manager
Punjab National Bank,
IT Procurement Department,
I.T. Division, HO: 5 Sansad Marg,
New Delhi 110 001

Please note that **HASH SUBMISSION and BID RE-ENCRYPTION** is a mandatory activity, failing which bidder will not be able to submit the bid. For details you may visit our e-Procurement Site https://etender.pnbnet.in.

Kindly also note that hard Copy of Technical Bid will be received only after successful Hash Submission and Online bid Re-encryption.

15. MODIFICATION AND/OR WITHDRAWAL OF BIDS

Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids. No bidder shall be allowed to withdraw the bid, if bidder happens to be successful bidder. In case of any deviation in the bid submitted in Online portal and the hard copy bid, the one submitted online will be considered and will be evaluated.

16. CONTACTING THE PURCHASER

Any effort by a bidder to influence the Purchaser in evaluation of the purchaser's bid, bid comparison or contract award decision may result in the rejection of the Bidders' bid. Purchaser's decision will be final and without prejudice and will be binding on all parties.

Bidders are also advised not to indulge in any unnecessary meetings or communications with Bank Officials. Any information necessary for the bidders will be communicated to them through e-mails.

17. TERMS AND CONDITIONS OF THE BIDDING FIRMS

The bidder has to accept all terms and conditions of the Bank and should not impose any of its own conditions upon the Bank. A bidder who does not accept any or all conditions of the Bank shall be disqualified from the selection process at any stage as deemed fit by the Bank.

18. LOCAL CONDITIONS

The bidder must acquaint himself with the local conditions and factors, which may have any effect on the performance of the contract and / or the cost.

19. PURCHASERS RIGHT TO ACCEPT OR REJECT ANY BID OR ALL BIDS

The Purchaser reserves the right to accept or reject any bid and annul the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bidder or bidders about the grounds for the purchaser's action. The Purchaser reserves the right to accept or reject any technology proposed by any bidder.

20. OPENING OF BIDS

The Date, time and location of bid opening is as per the tender schedule. Any change in Date, time or location of bid opening will be communicated to the participating bidders through e-mail. The technical bids will be opened in the presence of representatives of the bidders who choose to attend. In the event of the specified date of bid opening being declared a holiday for purchaser, the bids shall be opened at the specified time and place on next working day.

21. CLARIFICATIONS OF BID

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the bidder for clarification and response shall be submitted in writing, duly signed & stamped by the authorized signatory and no change in the price or substance of the bid shall be sought, offered or permitted. The clarification and response received from bidder will be subsequently part of bid submitted by that bidder.

22. PRELIMINARY EXAMINATION

The Purchaser will examine the bids to determine whether they are complete, whether any computational errors have been made, whether required information have been provided as underlined in the bid document, whether the documents have been properly signed, and whether bids are generally in order.

Arithmetical errors will be rectified as follows:

- If there is any discrepancy in total amount and multiplication of unit rate and Multiplication factor, unit rates will prevail and the total amount shall be recalculated on the basis of Unit rate and multiplication factor.
- If there is any discrepancy between words and figures, the amount in the words will prevail.
- AMC/ATS amount, if asked for in specified range, and quoted under or beyond the specified range, would also be recalculated.

The bid determined as not substantially responsive will be liable for rejection by the purchaser and may not be made responsive by the bidder by correction of the non-conformity. The decision of the Bank in this regard will be final.

The purchaser may waive any minor informality or non-conformity or irregularity in a bid, which does not constitute a material deviation, provided such waiver does not prejudice to affect the relative ranking of any bidder.

23. REVELATION OF PRICES

The prices in any form or by any reasons should not be disclosed in the technical or other parts of the bid except in the indicative commercial bid. Failure to do so will make the bid liable to be rejected.

24. EVALUATION AND AWARD CRITERIA

After opening of the technical bids, all the documents and annexure (except commercial documents/offer) will be evaluated first by the Bank.

First Stage: (Technical Evaluation)

1. Bid document must be submitted in a single hard bound file. (No loose pages must be submitted). **All pages of the Bid Document must be serially numbered and must be signed in Full (no initials) by the authorized signatory and stamped by Bidder's Official seal.** All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party. All documents, addressed to the Bank, should be submitted in Original. (No Photocopies will be acceptable).

2. All third party documents must be signed by their authorized signatory and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder is also required to substantiate whether the person signing the document is authorized to do so on behalf of his company. Inability of the bidder to prove the genuineness/authenticity of any third party document may make the bid liable for rejection.

3. Technical bid opening will be done in presence of authorized representatives of all the bidders (if they choose to be present) who have submitted technical bid successfully (both online & in Hard Bound File) within the stipulated time lines set by the Bank.

4. First of all, the RFP Cost and EMD of all bidders will be verified. If any RFP Cost/EMD is not found in order, that bidder will be declared ineligible for further participating in the tender process.

5. After that technical bids will be evaluated based on the eligibility criteria defined in the RFP document. Bids complying with all the eligibility criteria and confirming compliance to all the terms & conditions of RFP document would be further evaluated on technical parameters.

6. Bidders satisfying the technical requirements as determined by the Bank and accepting the terms and conditions of this document shall be short-listed for further process.

7. PNB will determine to their satisfaction whether the bidder selected as having submitted the best evaluated responsive bid is qualified to satisfactorily perform the contract. The decision of PNB will be final in this regard.

8. The Bank reserves the right to accept or reject any product/ item/ technology/ module/ functionality proposed by the bidder without assigning any reason thereof. The Bank also reserves the right to reject any Bid, in case any of the Technical Specification is not in compliance to Bank's requirement. Decision of the Bank in this regard shall be final and binding on the bidders.

Second Stage: (Commercial Evaluation)

In the second stage, the COMMERCIAL BID of only those bidders will be opened who will comply with all the eligibility criteria and confirm compliance to all the terms & conditions and technical specifications of the RFP document.

1. The commercial bids shall be opened in the presence of shortlisted bidders, if they choose to be present. The intimation of time and place of opening of commercial bids will be informed separately to the shortlisted bidders only. If the shortlisted bidders or their duly authorized representatives are not present, the commercial bids will be opened in their absence. No information regarding the Commercial opening will be provided later to the bidders who did not attend the commercial opening, neither telephonically nor through mail.

2. After opening of commercial bids as above, commercial evaluation & verification of the bids will be done by the Bank. Any arithmetic errors will be rectified as per clause 22-Preliminary Examination.

3. The bidders will be required to quote for all the items required by the Bank.

4. **Price Variation Factor**
   i) "If a bidder quoting higher prices, higher by more than 40% as compared to the average quoted prices (of all technically qualified bidders) for all items in aggregate, the same bidder shall not be called for reverse auction process". If due to such price variation factor, a bidder is not found eligible to be called for reverse auction and only one bidder is left commercially eligible, in such a situation, Bank reserves the right to negotiate with the L1 bidder.

   ii) Price variation Factor shall be considered collectively for both the solutions i.e for table C.

   iii) Price variation (both high or low) may also be considered for any particular solution/item i.e. bidder quoting abnormally high or abnormally low prices against any solution/item/s may also be liable for rejection.

The L-1 price and L-1 vendor will be decided on the basis of least total cost of both the solutions i.e Total of Table C of Annexure-XIII , derived after conducting reverse auction.

25. REVERSE AUCTION

Bank will hold Reverse Auction in the event of two or more bidders are commercially eligible. Final Item wise price shall be arrived after Reverse Auction. The procedure for the same is available on our e-procurement website. Reverse Auction/s will be conducted on mandatory items only **(Table-C of Indicative Commercial bid format (Annexure XIII))**. Base Price, Bid decrement value will be as per Bank's Discretion and will be communicated to all commercially eligible bidders only for seeking acceptance.

It will be mandatory for all the bidders to quote rates of all optional components that are required as per RFP. The rates of optional items will be negotiated with the successful bidder only.

a. If the commercially eligible bidders do not accept the base price and bid decrement value fixed by the Bank within the stipulated time given by the Bank, in such a situation Bank reserves the right to disqualify that/those bidder(s) from further RFP process.

b. After giving the acceptance by bidder(s) for the base price and decrement value, if the bidder(s) do not login in Bank's E-Auction portal during the Reverse Auction or refuse to participate in Reverse Auction at any time thereafter, then the bidder(s) will automatically get disqualified for further RFP process.

c. During the course of Reverse Auction if eligible bidders accept the base price and do not place any bid below the accepted base price after logging into the Reverse Auction portal, then out of these bidders, the one who has quoted least total price in Table-C of Indicative Commercial bid format (Annexure XIII) shall be treated as L1 bidder and Bank reserves the right to further negotiate with L1 bidder and finalize the final prices.

In case of any situation where Bank is left with only one eligible bidder, then Bank reserves the right to negotiate with that bidder and final Item wise price shall be arrived.

26. CONTACTING BANK OR PUTTING OUTSIDE INFLUENCE

Bidders are forbidden to contact Bank or its Consultants on any matter relating to this bid from the time of submission of commercial bid to the time the contract is awarded. Any effort on the part of the bidder to influence bid evaluation process, or contract award decision may result in the rejection of the bid.

27. CANCELLATION OF BID/ BIDDING PROCESS

PNB reserves the right to accept or reject any bid and annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the ground for its action.

28. DELAY IN THE SUPPLIER'S PERFORMANCE

Delivery of the goods and performance of the Services shall be made by the supplier in accordance with the time schedule specified by Bank.

29. GOVERNING LAW AND DISPUTES

All disputes or differences whatsoever arising between the parties out of or in relation to the construction, meaning and operation or effect of these Tender Documents or breach thereof shall be settled amicably. If, however, the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the Arbitration and Conciliation Act 1996, and the award made in pursuance thereof shall be binding on the parties. The Arbitrator/Arbitrators shall give a reasoned award. Any appeal will be subject to the exclusive jurisdiction of courts at Delhi.

The bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or the umpire, as the case may be, obtained. The venue of the arbitration shall be Delhi.

30. USE OF CONTRACT DOCUMENTS AND INFORMATION

The bidder shall not, without the Banks prior written consent, make use of any document or information provided by the Bank or otherwise except for purposes of performing contract. Successful bidder will have to sign Bank's approved Non-Disclosure Agreement (NDA).

31. CONFIDENTIALITY

The bidder shall not, without the written consent of the Bank, disclose the contract or any provision thereof, any specification, or information furnished by or on behalf of the Bank in connection therewith, to any person(s).

The bidder shall not, without the prior written consent of the Bank, make use of any document or information except for purposes of performing this agreement.

32. PATENTS RIGHTS

The supplier shall indemnify the purchaser against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.

- The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.
- The supplier shall expeditiously extinguish any such claims and shall have full rights to defend itself there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible therefore, including all expenses and court and legal fees.
- The Bank will give notice to the Supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.
- The Supplier shall grant to the Bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including-all inventions, designs and marks embodied therein in perpetuity.

33. ASSIGNMENT

The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the Purchaser's prior written consent.

34. FORCE MAJEURE

Notwithstanding the above provisions, the successful bidder shall not be liable for penalty or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the contract is the result of an event of force majeure. For purposes of this clause, "force majeure" means an event beyond the control of the bidder and not involving the bidders‟ fault or negligence and not

foreseeable. Such events may include, but are not restricted to, war or revolution and epidemics. If a force majeure situation arises, the bidder shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, the bidder shall continue to perform its obligation under the contract as far as is reasonably practical, and shall seek all reasonable alternative means of performance not prevented by the force majeure event.

35. NON DISCLOSURE

By virtue of Contract, as and when it is entered into between the Bank and the successful bidder, and its implementation thereof, the successful bidder may have access to the confidential information and data of the Bank and its customers. The successful bidder will enter into a Non-Disclosure Agreement to maintain the secrecy of Bank's data as per following:-

- That the successful bidder will treat the confidential information as confidential and shall not disclose to any third party. The successful bidder will also agree that its employees, agents, sub-contractors shall maintain confidentiality of the confidential information.

- That the successful bidder will agree that it shall neither use, nor reproduce for use in any way, any confidential information of the Bank without consent of the Bank. That the successful bidder will also agree to protect the confidential information of the Bank with at least the same standard of care and procedures used by them to protect its own confidential Information of similar importance. Without limitation of the foregoing, the successful bidder shall use reasonable efforts to advise the Bank immediately in the event that the successful bidder learns or has reason to believe that any person who has had access to confidential information has violated or intends to violate the terms of the Contract to be entered into between the Bank and the successful bidder, and will reasonably cooperate in seeking injunctive relieve against any such person.

- That if the successful bidder hires another person to assist it in the performance of its obligations under the Contract, or assigns any portion of its rights or delegates any portion of its responsibilities or obligations under the Contract to another person, it shall cause its assignee or delegate to be bound to retain the confidentiality of the confidential information in the same manner as the Bidder is bound to maintain the confidentiality. This clause will remain valid even after the termination or expiry of this agreement.

- That the successful bidder will strictly maintain the secrecy of Bank's data.

36. INDEMNITY

The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes except GST and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidder's obligation under these general conditions or for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of contract. Where any patent, trade mark, registered design, copyrights and/ or

intellectual property rights vest in a third party, the bidder shall be liable for settling with such third party and paying any license fee, royalty and/ or compensation thereon. In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the machine supplied by the bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidder's cost against such third party's claim and / or actions and against any law suits of any kind initiated against the Bank.

ANNEXURE I

TERMS AND CONDITIONS

1. SIGNING OF CONTRACT

The successful bidder(s) shall mandatorily enter into a Service Level Agreement (SLA), Non-Disclosure Agreement (NDA) and integrity Pact (IP) with Bank, within 30 working days of the award of the tender or within such extended period as may be permitted by the Bank. The letter of acceptance and such other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work in accordance with the Bid and the acceptance thereof, with terms and conditions shall be contained in a Memorandum of Understanding to be signed at the time of execution of the Form of Contract. If the contract is not signed within the given period (30 working days), the EMD will be forfeited after a grace period of 15 working days.

The bidder has to accept all terms and conditions of the Bank and should not impose any of its own conditions upon the Bank. A bidder who does not accept any or all conditions of the Bank shall be disqualified from the selection process at any stage as deemed fit by the Bank.

2. DURATION OF CONTRACT

Bank will enter into contract initially for a period of 5 years (3 years warranty plus 2 years ATS/AMC) for both the Solutions from the date of installation of all the hardware & software licenses at DC & DR, with option of further extension of contract, for another two terms of 1 year each, at the same rate and same terms & conditions, provided services of the bidder is satisfactory and at Bank's sole discretion.

Bank reserves right to cancel the contract at any time in case any of the two solutions fails to meet any of the requirements as mentioned in the RFP.

3. PERFORMANCE BANK GUARANTEE

The successful bidder has to submit the Performance Bank Guarantee (PBG), detailed as under:

a) The successful bidder will have to submit Performance Bank Guarantee amounting to 10 % of Total Purchase Order value, within one month of acceptance of purchase order & valid for a period of **5 years plus 6 months** from the date of entering into contract.
b) The Bank Guarantee should be issued by any Public Sector Bank or scheduled Commercial Bank other than Punjab National Bank.
c) The Performance Bank Guarantee will be furnished for due performance of the complete solution.
d) In case vendor submits any false information or declaration letter during the tender process or period of rate contract, Bank shall invoke the EMD/ Performance Bank Guarantee submitted by the bidder to recover penalty/damages. In case vendor fails to perform the contract, Bank shall invoke the Performance Bank Guarantee to recover penalty/damages.
e) No interest on PBG will be paid by Bank.

4. ACCEPTANCE OF ORDER (ORDER PLACEMENT)

Orders will be placed by the respective HO Division/Department. The vendor (successful bidder) shall have to accept and acknowledge orders within 15 working days from the date of order placement. Bank has a right to cancel the order and forfeit the entire EMD amount if the same is not accepted within a period of 15 working days from the date of order, otherwise it will be considered as accepted.

5. NOT ACCEPTANCE/ NON EXECUTION OF ORDER

In case the bidder shortlisted through this RFP process (hereinafter called "vendor") refuses to accept / execute the order, Bank will procure the same from the respective OEM as per existing terms & conditions and rate accepted by OEM. The said vendor will have to bear the difference of cost if any of such item / product purchased by Bank from OEM (Bank is having all the rights to recover the difference/ penalty amount from PBG as well as any amount payable to the said vendor). Bank also reserves the right to blacklist/debar the said vendor in such eventuality without giving any notice thereof in this regard for a period of further three years from the date of blacklisting/debarment.

6. DELIVERY& INSTALLATION

Bidder shall be responsible for delivery and installation of the complete solution (hardware & software both) ordered at both DC & DR site for both the solutions, within 6 weeks from the date of Purchase order. Installation means mounting of Servers in Rack (If any) and "Power-On" all the hardware with all the accessories provided with the hardware. The point of delivery/ destination will be as defined by the Bank in the purchase order.
The date on which the complete system is installed will be taken as the date of installation. In case of part installation of the system, the date of last items installed will be taken as the date of installation.

7. IMPLEMENTATION

Bidder shall be responsible for complete implementation, as per Scope of work & technical specification, of both the solutions at both DC & DR as well as test set up at DC within 1 months from the date of delivery or within 2 months from the date of Purchase Order, whichever is later.

8. ACCEPTANCE TEST

All the delivered hardware items may be subjected to an acceptance test. Vendor has to arrange one Engineer at the site at the date and time mentioned by the Bank to assist in the acceptance test.

9. PAYMENT

Payment will be made individually for both the solutions as per the following schedule: -

A-Total Hardware Cost
B-Total Software Cost including all required licenses
C-Implementation Cost including all required integrations
D-OTS Cost

Deliverables	**Eligible Amount**
Complete Installation of all the required hardware & delivery of all software licenses(Complete BOM at DC & DR)	70% of (A+B)
Sign Off of complete solution with all	(20% of A) + (20% of B) + (90% of C)

modules/functionalities	
After three months of sign-off	10% of (A+B+C) or immediately on submission of equivalent amount of BG
ATS/AMC	On Quarterly basis in arrears
OTS (Onsite Technical Support) Cost	On Monthly basis in arrears

NOTE: 100% of any item is the eligible amount after deduction of Penalty , if any.
In case of delayed delivery or incorrect delivery, then date of receipt of the correct and final component shall be treated as delivery date for penalty and other calculation. Bidder shall quote all the figures in numbers followed by total in words in the indicative commercial bid.
Further, the above payments will be released only after submission of PBG and signing of SLA (including Do & Don't), IP and NDA by Successful Bidder.

**** Cost of the project and its components shall remain the same during the contract period.***

***** Sign off will be given only after successful implementation as per the scope of work, submission of implementation certificate by the OEM & testing of the solution deployed in our Bank.***

10. INSURANCE

The hardware/equipment to be supplied under the contract period shall be fully insured till installation of the system by the bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation. Bank will not be responsible for any loss to bidder on account of non-insurance to any equipment or services. All expenses towards insurance shall be borne by the vendor.

11. WARRANTY

Both the solutions (both hardware and software) supplied should be covered under comprehensive on-site BACK-TO-BACK warranty for **three years** from the date of installation. Bidder should make adequate arrangements with OEM for the same. This includes replacing the faulty component, updating the latest patches of software, re-configuration, redeployment of application (if required), providing latest version (software subscription) of the software/license etc. Definition update / patch update, upgrade would be done by vendor immediately for critical updates or on monthly basis for normal updates/upgrades.
The vendor shall be fully responsible for the warranty of all equipment, accessories, spare parts, including that of software items etc. against any defects arising from design, material, manufacturing, workmanship or any act or omission of the manufacturer and/or vendor any defect that may develop under normal use of supplied equipment during warranty period.
Warranty should cover the following at no extra cost to Bank:-

- Service support should be available on 24 x 7 x 365 basis.
- Any issue except hardware failure in the deployed solution should be resolved within 4 hours of receipt of complaint.
- In case of failure of any hardware, replacement should be within 24 hours from the time call is lodged during warranty and AMC. The replacement unit has to be shipped by the OEM & should be compatible and the bidder should install and configure the same. Once confirmed by Bank on the successful working of the device, the faulty unit has to be collected by the bidder and delivered to OEM. All charges, including taxes if any, towards replacement has to be borne by the bidder.

- Any corruption in the software or media shall be rectified during the full period of the contract including Warranty and AMC.
- Warranty would cover updates/maintenance patches/bug fixes (available from the original software vendor) for system software & firmware patches/bug fixes, if any, for hardware.
- The vendor should provide on-site preventive maintenance on regular interval i.e. quarterly. Pro-active product health status check-up (on-site) and submission of report quarterly. During the preventive maintenance the bidder should also check the firmware / operating system running on the DAM servers and other components and upgrade the same to latest version as released by OEM. The vendor will be required to forward to the Banks well in advance (at least 7 days) the preventive maintenance schedule / plan to enable the Bank to intimate the locations/offices and obtaining downtime etc.
- Free of cost version upgrade/customization will be done by bidder whenever new version of firmware/software is released or new requirements comes.
- The bidder to note that, the Bank reserves the right to modify/update the parameter files/configuration after feasibility check by the vendor. The feasibility of same should be informed to the Bank.
- The bidder to submit detailed Root Cause Analysis for hardware & software related issues/failures.
- Any coordination with the OEM for support should be carried out by the bidder engineer.
- The bidder to note that, only under exceptional conditions remote access for devices would be provided. Under all other circumstances bidder to provide on-site support only.
- The OEM must provide technical support. The OEM must provide the dedicated login credentials to Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. Bank should be able to raise tickets directly to OEMs.
- Bank should have a facility to log a call using web interface wherein all the support contract details should be linked. This interface should provide the incident number for monitoring the progress of the call/support ticket. The Bank should also have flexibility to log the calls using either emails/telephone also.
- The OEM should have a comprehensive known error database or knowledge database in the form a web access which is accessible to Bank team for resolving first level issues. This is not a local database maintained to track incidents. This repository is the knowledge base of all the incidents resolved worldwide by the vendor support teams.

12. ANNUAL MAINTENANCE CONTRACT (AMC)/ANNUAL TECHNICAL SUPPORT (ATS)

The On-site, comprehensive BACK-TO-BACK AMC/ATS (quoted in percentage) will be valid for a period of **two years** after expiry of three year's warranty period and the quoted %age will be continued for entire contract period. Bidder should make adequate arrangements with OEM for the same. The scope of AMC is same as Warranty. Payment of AMC and ATS will be released on quarterly basis. The AMC/ATS may be terminated by the Bank after giving three months' notice in case of deficiency in services. Bank may extend the AMC/ATS term for two terms of 1 year each on same rates and same terms and conditions.

The quoted percentage (%) for AMC and ATS would be applicable for proactive support on 24 x 7 x 365 basis. AMC and ATS would cover all components of the offered appliance without any exceptions.

The Bank will enter into an all-inclusive Annual Maintenance Contract (AMC) with the selected bidder after the expiry of respective warranty period for the hardware item and software systems.

The scope of AMC will be same as scope of Warranty mentioned in above Para.

13. UPGRADES AND UPDATES

The bidder shall be required to provide all future updates and upgrades for the proposed hardware/software provided free of cost during contract period. If however, the upgrades/updates is not available then the support for the implemented solution should be available at any point of time.

14. PENALTY CLAUSE

Penalty will be deducted individually for both the solutions as per the following schedule:

14.1 Penalty due to delay in Services

A-Total Hardware Cost
B-Total Software Cost including all required licenses
C-Implementation Cost including all required integrations

S.N	Item	Expected Timeline	Penalty	Max. Penalty	Threshold of Delay
1	Delivery of Complete Solution including hardware	Within 4 weeks from the date of Purchase Order	1% of (A+B) for every week delay	10% of (A+B)	6 weeks from the date of PO
2	Complete Implementation	Within one months from the delivery or within two months from the date of Purchase Order, whichever is later.	1% of (A+B+C) for every week delay	10% of (A+B+C)	three months from the date of PO

Bank reserves the right to Cancel the Purchase Order, Terminate the Contract, Forfeit the Performance Bank Guarantee and Blacklist the Vendor, in case the Vendor exceeds the threshold limit of Delay for any of the items above. Bank, at its sole discretion, may exercise any or all of the options against the Vendor, in such circumstances.

14.2 Penalty due to Downtime

After implementation of the Complete solution, Penalty will be deducted for downtime of the system (Hardware / Application failure) as below

Uptime (U)	Penalty
U >=99.95	No Penalty
99.50<=U< 99.95	0.1 % of (A+B)
99.00<=U< 99.50	0.2 % of (A+B)
98.50<=U< 99.00	0.3 % of (A+B)
98.00<=U< 98.50	0.4 % of (A+B)
And so on	For every 0.5 % drop in the Uptime, Penalty @ 0.1% of (A+B)

SLA will be monitored on Monthly basis.
Penalty due to downtime, during three years of warranty period will be deducted from **any** subsequent payment to be made to the Vendor.

Penalty due to downtime, during AMC/ATS period will be deducted from AMC/ATS payment.

14.3 Penalty due to Absence of Onsite Technical support(OTS)

During the Implementation period and 1 year post implementation- In the absence of the OTS (either bidder's resource or OEM's resource), suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.5% of the Implementation cost, for each day, upto a maximum of 10%.

If the Bank avails Onsite Technical support-The Bidder has to deploy resource within 15 days from the date of PO, failing which penalty @ 1% of OTS cost for each day, upto a maximum of 10%, would be deducted from any future payment due. In the absence of the engineer, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @1% of the OTS Cost, for each day, upto a maximum of 10%.

Penalty as in 14.1, 14.2 & 14.3 can be levied simultaneously. Maximum deducted penalty of one type will not affect any other type of penalty i.e. All the three types of penalties can be levied upto their maximum limit simultaneously.
Penalty will be levied individually for both the solutions and Maximum deducted penalty of any type on any of the solution will not affect any other type of penalty on the other solution.

15. SERVICE LEVEL AGREEMENT

The selected vendor will also have to enter into a Service level agreement for Service Support and Maintenance of complete solution as per the terms and conditions of the RFP and covering the scope of work and technical requirements.
The non-delivery of any services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP. The onsite engineers/representative deployed by the successful vendor will not claim any benefit from the Bank and any loss or damage to the Bank due to them will be the sole responsibility of the Vendor.

16. TAXES

The rates quoted in Performa for Indicative Commercial offer should be inclusive of all taxes except GST. However, GST shall be paid to the bidder on actual basis at the rate applicable. The rate of applicable GST should be informed and charged separately in the invoice generated for supply of the product.

17. CANCELLATION OF PURCHASE ORDER

After issuance of purchase order to successful bidder, Bank reserves the right to cancel the Purchase Order without giving any notice, for following reasons –

a) Non submission of acceptance of order within 15 working days of placement of Purchase Order.
b) Non submission of Performance Bank Guarantee within stipulated time as specified in the RFP.
c) Non signing of contract within the time specified by Bank.

18. SIGNING OF PRE CONTRACT INTEGRITY PACT

The bidder should submit Original Executed Integrity Pact along with the technical bid. The Integrity Pact must be executed on stamp paper of applicable value and must be signed by all the witnesses also. The Performa of Integrity Pact is as per (Annexure-XV)

19. DELAYS IN THE SUPPLIER'S PERFORMANCE

Delivery of the goods and performance of the Services shall be made by the supplier in accordance with the time schedule specified by purchaser. Any delay in performing the obligation by the supplier will result in imposition of liquidated damages and/or termination of rate contract for default.

20. INDEMNITY

The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes (except GST) and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidder's obligation under these general conditions or for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of purchase order. Where any patent, trade mark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liable for settling with such third party and paying any license fee, royalty and/ or compensation thereon.

In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the machine supplied by the bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidder's cost against such third party's claim and / or actions and against any law suits of any kind initiated against the Bank, Vendor (successful bidder) will also assume full responsibility of any loss or damage caused due to any of their onsite engineer/representative.

21. TERMINATION OF CONTRACT

The quality of services given by the bidder & progress of the project will be reviewed monthly and if the services are not found satisfactory, the Bank reserves the right to terminate the contract by giving 30 days' notice to the bidder, including 15 days curing period. The decision of the Bank regarding quality of services shall be final and binding on the bidder. The Bank shall have the right to terminate/cancel the contract with the selected bidder at any time during the contract period, by giving a written notice of 30 days, for any valid reason, including but not limited to the following :

a) Excessive delay in execution of order placed by the Bank or in providing mandatory training to Bank Officials.
b) Discrepancies / deviations in the agreed processes and/or products
c) Failure of vendor (successful bidder) to complete implementation of appliance within the time as specified in the RFP document
d) Violation of terms & conditions stipulated in this RFP.

e) Exceeding any of the threshold limit of Delay as per **clause 14.1** for any of the solution.

Notwithstanding anything contained hereinabove, the Bank reserves the right to terminate the contact at any time without assigning any reasons.
In case of termination of contract for the reasons that the services of vendor are not found satisfactory", the Bank shall be free to Blacklist the vendor thereby debarring them from participating in future Bids/Tender processes

22. GOVERNING LAWS AND DISPUTES

All disputes or differences whatsoever arising between the parties out of or in relation to the construction, meaning and operation or effect of these Tender Documents or breach thereof shall be settled amicably. If, however, the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the Arbitration and Conciliation Act 1996, and the award made in pursuance thereof shall be binding on the parties. The Arbitrator/Arbitrators shall give a reasoned award. Any appeal will be subject to the exclusive jurisdiction of courts at Delhi.

The bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or the umpire, as the case may be, is obtained.

The venue of the arbitration shall be Delhi. This is applicable to successful bidder only.

23. USE OF CONTRACT DOCUMENTS AND INFORMATION

The supplier shall not, without the Bank's prior written consent, make use of any document or information provided by Purchaser in Bid document or otherwise except for purposes of performing contract.

24. PATENT RIGHTS

The supplier shall indemnify the Purchaser against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.

- The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.
- The supplier shall expeditiously extinguish any such claims and shall have full rights to defend it there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible including all expenses and court and legal fees.
- The Bank will give notice to the Supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.
- The Supplier shall grant to the Bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including-all inventions, designs and marks embodied therein in perpetuity.

25. ASSIGNMENT

The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the Purchaser's prior written consent.

26. CONTRACT BETWEEN BANK AND SHORTLISTED BIDDER

The shortlist bidder shall be required to execute SLA (Service Level Agreement), IP (Integrity Pact) and NDA (Non-Disclosure Agreement) with the Bank.

27. PRINCIPAL TO PRINCIPAL RELATIONSHIP

The employees engaged by the Vendor shall be deemed to be the employees of vendor only, and the Bank shall not be connected with the employment or the terms and conditions thereof in any way. The Vendor alone would comply with the statutory obligations and Labour Regulations/ Rules in this regard. None of the provisions of this Agreement shall be deemed to constitute a partnership between the parties hereto, and neither party shall have authority to bind the other except as specifically provided for hereunder. Neither party hereto is the agent of the other and there is no master-servant relationship between the parties. The relationship is on principal to principal basis.

The Vendor shall be responsible for payments of all statutory dues with respect to each of its personnel/employees engaged by it to render service under this Agreement with respect to each applicable Labour law, including, the Minimum Wages Act, 1948, the Payment of Wages Act, 1936, the Payment of Bonus Act, 1965, the Employees' State Insurance Act, 1948, the Payment of Gratuity Act, 1972, the Maternity Benefit Act, 1961, the Employees' Provident Funds and Miscellaneous Provisions Act, 1952, etc. No dues/contributions under any labour legislations, as applicable, are payable by the Bank with respect to the Vendor's personnel/employees. The vendor will have no claims whatsoever against the Bank with respect to payment of statutory dues/contributions to personnel/employees of under applicable labour legislations.

28. LIMITATION OF LIABILITY

Vendor's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for

a) IP Infringement indemnity

b) Bodily injury (including Death) and damage to real property and tangible property caused by vendor/s' gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase orders placed by Bank on the vendor that gave rise to claim, under this tender. Vendor shall not be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order.

Date:_____
Place:_____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-II

UNDERTAKING FROM THE BIDDER

To,
The Asstt. General Manager
IT Procurement Department
Punjab NationalBank
I.T. Division, Head Office
New Delhi

Sir
Reg.: Our bid for RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

We submit our Bid Documents herewith**.**

We understand that

- You are not bound to accept the lowest or any bid received by you, and you may reject all or any bid.
- If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the purchaser to do so, a contract in the prescribed form. Till such a formal contract is prepared and executed, this bid shall constitute a binding contract between us and Bank.
- If our bid is accepted, we are responsible for the due performance of the contract.
- You may accept or entrust the entire work to one Bidder or divide the work to more than one bidder without assigning any reason or giving any explanation whatsoever.

Date:_____
Place:_____
Yours faithfully

Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-III

ELIGIBILITY CRITERIA OF THE BIDDER

S.N.	Eligibility Criteria	Supporting Documents to be submitted	Compliance (Yes/No)
1	The bidder should be registered with Registrar of companies/firms in India for atleast 5 years.	Certificate of incorporation or any other certificate of registration issued by competent authority from Government of India.	
2	Bidder and OEM must be an ISO 27001: 2013 or higher certified company.	ISO 27001: 2013 or higher certificate	
4	The proposed Network Anti-APT solution and Deception/Decoy Solution must have been implemented during the last 3 years as on date of RFP and currently running successfully, in atleast 1 PSU Banks/ Private Banks in India. *(One reference each for both the solutions is required)*	Satisfactory Performance Certificate from the Clients as per Annexure-VI. OR Purchase Order along with Email from the client containing all the required information. *Kindly note that that Client's Email should be from their official Email IDs only, containing their name, designation & Mobile no.* OR Copy Of Work Order along with Installation Certificate signed & stamped by the Client OR Copy of Work Order along with any other proof of execution. (*Kindly note that any of the above documents submitted must be sufficient enough to certify OEM's/bidder's experience, must be authentic and must also contain all the material information as required in Annexure-VI)*	
5	The bidder must have successfully implemented Anti-APT/ Deception/ Decoy/ Honeypot Solution during the last 3 years as on date of RFP in atleast 1 PSU Banks/ Private Banks/PSU/BFSI in India, which should be currently running successfully.		
6	The bidder and OEM should have Support center in Delhi/NCR and Mumbai.	Undertaking to be submitted	
7	The bidder should be the Original Equipment Manufacturer (OEM) of the offered solutions, with presence in India, or its authorized representative in India.	In case of authorized representative, MAF from OEM of both the Solution as per Annexure-X in their letter Head needs to be provided. In case the bidder is itself the OEM, undertaking as per Annexure-XI on their company's letter head should be provided.	
8	The bidder should have a minimum turnover of INR 20 crores (Rupees Twenty crores) per annum from Supply/Installation/Maintenance of IT Security Solutions in India, for the past 3 financial years i.e. 2015-16, 2016-17, 2017-18. The bidder should have positive networth during the last three financial years.	Provide CA Certificate as per Annexure-IX and Audited Financial statements (Balance sheet & Profit & Loss statement) for the last three (3) Financial years. The CA certificate provided in this regard should be without any riders or qualification,	
9	The bidder should not be involved in any litigation which threatens	Certificate is to be provided by the chartered accountant/statutory auditor,	

	solvency of company.	as per Annexure- VII	
10	Bidder should not have been black listed by the Government / Government agency / Banks / Financial Institutions in India during last 3 years. Self Certificate/Undertaking is to be provided.	Undertaking to be provided as per Annexure-VIII	
11	Labour Law Compliance	Undertaking to be submitted	

NOTE:

1. For a particular Solution, only the OEM or its authorized representative can bid. If both the OEM and its authorized representative bid for the same Solution, both the bids will be rejected.
2. If any Solution of Principal / Original Equipment Manufacturer (OEM) is being quoted in the tender, the OEM Company cannot bid for any other OEM's product.
3. In case of Indian Authorized Representative (IAR) / Agent / System Integrator (SI), maximum two Authorized Representatives of a particular Principal or Original Equipment Manufacturer (OEM) / Solution Provider can participate in the tender process.
4. In case any purchase order has been issued to the bidder by the Bank in respect of any other project/product and the same has not been delivered/executed even after the prescribed time period and is pending for execution as on date of bid, the bid of the respective bidder is liable for rejection.
5. Bidder should submit detailed response along with documentary proof for all of the above eligibility criteria. The eligibility will be evaluated based on the bid and the supporting documents submitted. Bids not meeting the above eligibility criteria will be rejected.
6. Technical Evaluation will be done by Bank's technical evaluation committee and the decision of the committee will be final.
7. Bidders to submit relevant documentary evidence for all parameters mentioned.
8. Providing any wrong information by the bidder will result in disqualification of the bidder. The Bank may cross check above parameters by any means / during site visit.
9. All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party. All documents, addressed to the Bank, should be submitted in Original. (No Photocopies will be acceptable).
10. All third party documents must be signed by their authorized signatory and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder is also required to substantiate whether the person signing the document is authorized to do so on behalf of his company. Inability of the bidder to prove the genuineness/authenticity of any third party document may make the bid liable for rejection.

Date: _____
Place: _____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-IV

BIDDER'S INFORMATION

S. N.	Information	Particulars / Response
1	Company Name	
2	Constitution	
3	Date of Incorporation	
4	Company Head Office Address	
5	Registered office address	
6	GST No.	
7	Whether MSME(quote registration no. and date of registration, copy to be attached)	
8	Whether bidder eligible for preference to domestically manufactured electronic products (DMEP) in government procurement vide notification dated 23.12.13 and guideline dated 16.11.15 as amended from time to time and updated in ministries web site – www.deity.gov.in/esdm/pmn as applicable to the Bank.	
9	Bank Account Detail:Account Number, Account Name, IFSC, Bank Name	
10	Name, Designation, Tel. No, E-Mail of the authorized signatory submitting the RFP (Please enclose the copy of board resolution)	
11	Specimen Full signature	
12	Contact persons address, telephone number, mobile number, Fax Number, E-Mail ID. (give at least 2 contact persons details)	
13	Details of Service Support Center in Delhi/NCR and Mumbai	Complete Address: No. of Support Engineers: Contact Person (Name & No.): Email ID:
14	Whether company has been blacklisted for service deficiency in last 3 years. If yes, details thereof.	
15	Any pending or past litigation (within three years)? If yes please give details	Yes/No/Comments (if option is 'Yes')
16	Please mention turnover for last three financial years and include the copies of Audited Balance Sheet in support of it.	**FY** / **Turnover Rs.(in Cr)** / **Net Profit/Loss Rs. (in lacs)** / **Net Worth Rs. (in Cr)** **2015-16** **2016-17** **2017-18**

Date: _____
Place: _____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE V

COMPLIANCE STATEMENT

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

DECLARATION

Please note that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. Bank reserve the right to reject the bid, if bid is not submitted in proper format as per RFP.

Compliance	Description	Compliance (Yes/No)
Terms and Conditions	We hereby undertake and agree to abide by all the terms and conditions including all annexure, corrigendum(s) etc. stipulated by the Bank in this RFP. (Any deviation may result in disqualification of our bid).	
Scope of work and/ Technical Specification	We certify that the systems/services offered by us for tender conform to the Scope of work and technical specifications stipulated by you. (Any deviation may result in disqualification of our bid).	
RFP, Clarifications & subsequent Corrigendum/s , if Any.	We hereby undertake that we have gone through RFP, clarifications & Corrigendum/s issued by Bank and agree to abide by all the terms and conditions including all annexure, corrigendum(s) etc. stipulated by the Bank in this RFP. (Any deviation may result in disqualification of our bid).	

Date: _____
Place: _____

Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company

PERFORMANCE CERTIFICATE

To be provided on letter head of the issuing Bank

The Asstt. General Manager
IT Procurement Department
Information Technology Division
Punjab National Bank
Head Office, 5 Sansad Marg
New Delhi – 110 001

Sir,

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) /Deception/Decoy Solutions.

This is to certify that M/s _____ has supplied/implemented _____ solution which is a Network Anti- Advanced Persistent Threat (N/w-Anti-APT) Solution/Deception Solutions originally developed by _____(OEM name) to our organization since_____. The solution is currently running successfully.

The services of M/s_____are satisfactory.

The certificate has been issued on the specific request of the company.

Date: _____
Place: _____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Bank

ANNEXURE – VII

LITIGATION CERTIFICATE

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

To be provided by Statutory Auditor/Chartered Accountant

This is to certify that M/s_____, a company incorporated under the companies act, 1956 with its headquarters at, _____ is not involved in any litigation which threatens solvency of the company.

Date: _____
Place: _____

Signature of CA/Statutory Auditor

Name of CA/Statutory Auditor:
Designation:
Seal of Company
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE –VIII

UNDERTAKING FOR NON- BLACKLISTED

To be provided on letter head of the Bidder's Company

The Asstt. General Manager
IT Procurement Department
Information Technology Division
Punjab National Bank
Head Office, 5 Sansad Marg
New Delhi – 110 001

Sir,

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

We M/s_____, a company incorporated under the companies act, 1956 with its headquarters at, _____ do hereby confirm that we have not been blacklisted/ debarred by the Government / Government agency / Banks / Financial Institutions in India during last 3 years.
This declaration is been submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,
Yours faithfully,

Date: _____
Place: _____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-IX

TURNOVER CERTIFICATE

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

To be provided by Statutory Auditor/Chartered Accountant

This is to certify that M/s_____, a company incorporated under the companies act, 1956 with its headquarters at, _____ has the following Turnover, Net Profit/Loss and Networth from its Indian Operations out of which turnover of Rs._____is from Supply/Installation/Maintenance of IT Security Solutions in India, for the past 3 financial years i.e. 2015-16, 2016-17, 2017-18.

This information is based on the Audited Financial Statements for 2015-16,2016-17 and 2017-18.

Financial Year	Turnover (in Rs.)	Net Profit/Loss (in Rs.)	Net Worth (in Rs.)
2015-16			
2016-17			
2017-18			

Date: _____
Place: _____

Signature of CA/Statutory Auditor
Name of CA/Statutory Auditor:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-X

MANUFACTURER'S (OEM) AUTHORIZATION FORM (MAF)

(To be provided on the Letter head of the OEM duly signed & stamped by their Authorized Signatory.)

To
The Asstt. General Manager
I T Procurement Department
Punjab National Bank
I.T. Division, Head Office
New Delhi

Sir

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) / Deception Solutions.

We hereby submit the following:-

1. We, M/s_____ are the OEM of _____(Name of the product/Solution/Hardware), being offered to Punjab National Bank through M/s _____(Bidder's Name), who is our authorized Partner/representative in India for supply of this Product/Solution/Hardware and we have the IP (Intellectual property) rights for the offered Solution.
2. We agree to provide services as per the scope of work and technical specifications of this RFP through our partner M/s _____
3. In case the bidder i.e. M/s _____ is not able to perform obligations as per RFP during the contract period (like if bidder ceases to exist from the ICT Industry, stops services or support to the Bank, terminates contract due any reasons with Bank or due to any other reason), we will perform the said obligations, as per given scope of work of RFP, either directly or through mutually agreed third party/any other authorized Partner of ours.
4. With reference to the all components/parts/assemble/software used inside the company products/Hardware being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly are being used or shall be used.
5. In case of default/unable to comply with above at the time of delivery or during installation, for the hardware / software already billed, we agree to take back the supplied items without demur, if already supplied and return the money if any paid to us by you in this regard. We also take full responsibility of both Parts & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.
6. We hereby further undertake to supply only new components and no refurbished or recycled components will be supplied.

Date:
Place:
Yours faithfully
Signature of Authorized Signatory
Name of Signatory:
Designation:
Seal of Company

ANNEXURE-XI

UNDERTAKING FOR BEING THE OEM OF THE OFFERED PRODUCT

To
The Asstt. General Manager
I T Procurement Department
Punjab NationalBank
I.T. Division, Head Office
New Delhi

Sir

Reg.: RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

We hereby submit the following:-

1. We, M/s_____ are the OEM of_____which is a Network Anti-Advanced Persistent Threat (N/w-Anti-APT) / Deception Solutions, being offered to Punjab National Bank through this RFP and we have the IP (Intellectual property) rights for the offered Solution.
2. We agree to provide services as per the scope of work and technical specifications of this RFP.
3. With reference to the all components/parts/assemble/software used inside the company products/Hardware being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly are being used or shall be used.
4. In case of default/unable to comply with above at the time of delivery or during installation, for the IT Hardware including hardware / software already billed, we agree to take back the supplied items without demur, if already supplied and return the money if any paid to us by you in this regard. We also take full responsibility of both Parts & Service SLA as per the content.
5. We hereby further undertake to supply only new components and no refurbished or recycled components will be supplied.

Date:
Place:
Yours faithfully
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company

ANNEXURE-XII

Technical specification of the Offered solution

(to be submitted in original by both the OEM and the bidder on their letter head, duly signed & stamped by their authorized signatory)

Network Anti-APT Solution

SN	Technical Specification	Compliance (Yes/No)	Remarks, if any
1	The Anti-APT solution should secure WEB downloads before they reach the Bank. Anti-APT solution should have full visibility of these SSL traffic and prevent from malicious web file download.		
2	The Anti-APT solution should secure incoming traffic with a single solution over multiple surfaces and vectors with the ability to scale up quickly. Multiple surfaces and vectors are as follows – a. Detect and prevent capabilities for both Web traffic b. Support SSL decryption/encryption for web traffic (through external appliance/within the appliance) c. Work in a highly scalable environment d. Be able to offload sandbox services to the appliance e. Be able to integrate with 3rd parties f. Be able to secure all vectors and surfaces g. Minimal use of devices h. Minimal to no impact of end user's experience i. Single management for all managed assets		
3	The solution should have visibility and analysis of malware threats and prevent and protect against malware and zero-day modern attacks and attack techniques including computers infected with bots, communications with CnC sites, viruses, and unknown malware (zero day attacks and malware that cannot be detected by traditional anti-virus systems). The solution should provide evasion-resistant malware detection, and comprehensive protection from unknown malware and the most dangerous zero-day and targeted attacks, while ensuring quick delivery of safe content to PNB users.		
4	The solution should be able to protect against Advanced Malware, zero-day web exploits and targeted threats without relying on signature database.		
5	The solution should be able to identify malware present in network file shares and web objects (For Eg:JPEG, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc. and any new formats having vulnerabilities to carry potential malware) and able to quarantine them.		
6	The solution should be able to block malware downloads over different protocols.		
7	Solution must not be dependent upon first detecting an initial malware infection (that often happens outside of a network) to identify a subsequent or related infection.		
8	The solution should recognize new variants of existing malware families and identify new families.		
9	The solution should have capability to fully reveal malware's current and potential payloads.		

10	The solution must be capable of Automated Malware Analysis, Real-Time Threat detection, Ransom ware detection, Dormant threat detection and C & C and Botnet detection that are carried by any protocol		
11	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.		
12	Solution should perform dynamic analysis of files outside of an Bank's network, in a space where malware files cannot evade detection. Specifically, malware files should be processed in a dedicated dirty space, with full Internet access that allows bare metal analysis of the malware, to counter VM and Internet aware malware as well as implement other controls (such as time dilation, key stroke counts, varying software configuration, etc.)		
13	Solution should provide a dynamic analysis option that does not allow for the possibility of malware attacks on other systems.		
14	Solution should identify system hooks, network communication, file accesses, file changes, etc. used by suspicious files charged with infecting a system. These malware-related traits and actions should be decipherable via the dynamic analysis of suspicious files.		
15	Solution should detect whether malware downloaded by an endpoint was effectively installed (executed) on the endpoint, this done via methodologies that do not utilize endpoint agents i.e. Agentless approach		
16	The proposed solution should be able to identify malware that has been packed or protected with Crypters, Packers		
17	The Solution should support the following multiple advanced malware analysis methods: a. AV Signatures b. Threat Reputation c. Signature-less engine d. Sandboxing e. Static Code analysis f. Dynamic Code analysis		
18	The solution should identify any logic bombs (time based execution delays) hidden in the malware waiting for a trigger to cause damage at a later time		
19	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific url, or changed the name of a running process to hide itself.		
20	The solution should quickly inspect and should discover malicious code at both the CPU and the operating system levels. Discovered malicious files should be prevented from entering the network.		
21	The solution must have the ability to scrub active content from documents type file providing the user documents with zero active content and deliver a safe copy of the file to the user.		
22	Solution should be able to Identify suspicious embedded object in document file like OLE & Macro extraction, Shell code & exploit matching and also the ability to detect and scan pdf files for embedded code.		
23	The Anti-APT solution should support multiple deployment options, providing a cost-effective solution. Files can be sent from existing gateways to an on premise appliance. As part of the already Installed security gateway, the solution should be applied across the entire		

	organization, or implemented only for specific individuals, domains, or departments.		
24	The solution should have visibility of high risk web applications and websites used by PNB employees such as: P2P File Sharing applications, Proxy anonymizers, File Storage applications, malicious websites, and more.		
25	The solution should have visibility of sensitive data sent outside the bank (PNB) via web.		
26	The solution should have visibility of downloads of malicious mobile applications, infected mobile devices, outdated mobile OS versions, access to high risk web applications and websites, usage of cloud base mobile apps		
27	The solution must not be a —point of failure in network traffic flow; the failure of one or more components of the solution should not affect the organizational network‘s functionality. i.e. Solution should work in pass through Mode /SPAN/ Mirror Traffic.		
28	Solution should be deployed on premise and along with on premise sandboxing capability where the objectionable content may be executed and inspected, of the following Operating Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2, Linux, Solaris10, Redhat 5 & Above, Unix and MAC OS, all industry standard OS. This requirement should be based on virtual execution and should not be Hardware or chipbased function.		
29	Solution should have option to upload custom sandbox image running in Bank’s environment.		
30	The sandbox must have the capability to analyze large files and must be able to support more than 50MB file size and following File type supports (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz,.tar.Z, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)		
31	The solution should support Sandbox test environment which can analyze threats to various operating systems, browsers, databases etc.		
32	The solution should have Infections detection without sandbox features as well.		
33	Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of file		
34	Solution must inspect SMTP, POP3, IMAP traffic, UDP traffic, Proxy/http traffic, DNS traffic, Non-standard TCP port traffic		
35	Solution should be capable to integrate with like Firewall/IPS/ Web Proxy/ Antivirus Solution/Mail Gateways/ Web gateways/Active Directory to enforce user based policies and to mitigate risk by blocking similar session.		
36	The solution should support discovery of infections via Ipv4 and Ipv6 Traffic Analysis		
37	Solution/appliance must have RAID redundancy (for hard drives), network redundancy (for management network interfaces), power Supply and Fan module redundancy.		
38	Hardware must have minimum 4 x 1G Ethernet ports and 4X10G Ports. SFP to be provided with the hardware. Hardware should have dedicated management port.		

39	Hardware should have minimum capacity of 4 TB		
40	The solution should identify infections regardless of the host‘s Operating System and devices used (OS- agnosticism)		
41	Solution should track the infection or threat history for a device, with the ability to access all forensic evidence for past infections. (6 months)		
42	The solution should support hostname resolution through either Net Bios Lookup or reverse DNS. (Asset Identification)		
43	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the Bank's network.		
44	The solution should be appliance based with hardened OS. No information should be sent to third party systems for analysis of malware automatically.		
45	The solution should be able to block the call back tunnel including fast flux connections.		
46	The solution should be able to pinpoint the origin of attack, Threat Description and help to understand the severity and stage of each attack.		
47	The solution should have a Centrally managed Dashboard with features to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, Attacked ports, Source hosts etc.		
48	The Dashboard should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.		
49	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through the dashboard.		
50	Solution should be able to capture and display all events (either in sequence or by event type) in a simple, intuitive interface to understand the contributing events to an infection.		
51	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.		
52	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.		
53	Solution should have built in reports such as: - Executive Reports - Incident Response Reports - Infection Life Cycle Reports - Malware in Motion Reports - System Health Reports		
54	The solution should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations		
55	The solution should be able to export event data to Bank‘s existing SIEM or Incident Management Systems		
56	Solution should be able to support XFF (X- Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment. The solution should provide support for inspection of XForwarder- For (XFF) information on HTTP traffic.		

57	The solution should be able to integrate with deployed appliances to share malware information/ zero day attacks knowledge base.		
58	The solution should be able to capture packets for deep dive analysis and should support remote packet capturing for Kerberos traffic from the remote location for analysis. The solution should store packet captures (PCAP) of all Malicious communications detected by sandbox and should have the ability to capture, publish and download PCAP files.		
59	Solution must be easily scalable to support monitoring a large number of devices and bandwidth with throughput support commensurate with Bank's networks.		
60	Management access and inter-system communication must be handled in a secure fashion (no http, no ftp, tftp, etc.)		
61	Solution should identify infections • through corroboration of Suspicious Network Communications Identified through Behavioural, Content, and Source/Destination Analysis • on victim machines with corroborated evidence (not just alerts), without needing to interact directly with the host (victim) device. • beyond just the initial dropper and be able to identify successful communicated to C & C server and successful malware execution on Endpoint. • for devices that are mobile (outside of network perimeter defences) on split-tunnel VPN connections. • regardless of the host's Operating System and devices used. • using P2P Malicious Communications such as Zero Access, TDL4, Zeus V3, and Sality (The solution should identify such malicious softwares like Sality, etc.) • without seeing the malware samples and without any file analysis features.		
62	Solution should provide administrators with the ability to view file download activity associated with infected Endpoint for a window of time prior to the determination of the endpoint's infected status.		
63	Solution must be able to handle minimum of 4 Gbps of traffic capacity for inspection		
64	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.		
65	Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall and IDS/IPS		
66	The Proposed solution should have capability to detect attacker behaviour within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..)		
67	The proposed solution should provide Geo location intelligence for (malware sources, network exploit sources, document exploit sources, malware c&c destinations) and should control traffic based on geographical locations.		
68	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance threats.		
69	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.		

70	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.		
71	Solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.		
72	Solution should be able to support up to 5 network segments on a single appliance.		
73	Solution should be able to identify and help understand the severity and stage of each attack.		
74	Solution should have built in capabilities to add exceptions for detections.		
75	Solution should have capabilities to configure files, IP, URLs and Domains hashes to Black list or white list.		
76	The proposed solution should support Multiple protocols inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device		
78	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.		
79	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis and to correlate the detections on the device itself.		
80	Solution should correlate events and differentiate between a confirm infection and a suspicious event, thereby pinpointing infected devices accurately.		
81	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.		
84	Solution should identify Domain Generation Algorithm (DGA)-based crime ware.		
85	Solution should identify TOR or DNS Tunnelling to conceal their communications		
86	Solution should support detection of DNS Query for malicious domains.		
87	Solution must have the ability to track and trace all C&C communications negotiated by a threat, not only the initial one-sided —call-back of a dropper.		
88	Solution should support inspection of evidences both per threat and per asset.		
89	Solution should provide a conviction engine that aggregates evidence and determines the presence of a threat on a device.		
90	Solution must include intelligence about malicious files seen globally and not only from within the local network		
91	The solution should indicate the degree of certainty the solution has of threat presence on a device; it should not just alert in discriminately		
92	Solution should provide risk ranking of an infection to a network, based on the activity of the threat locally within the network (frequently of malicious communication attempts, data transferred, importance of infected device).		
93	The solution should allow administrator-level users to include custom threats (used for testing purposes) that can be created and tracked via the User Interface. Custom threat can be created based on domain, IP		

	Address and MD5 Hash. Custom threats are to be tried only in test environment.		
94	Solution should include automated real time intelligence updates.		
95	Solutions should allow for incidents to be marked, tagged and acknowledged and should be able to mark assets/host		
96	Solutions should allow a user to track investigation efforts at an asset/device level by supporting tagging/notes, marking assets and threats as remediated, and support auto-expiration if no further evidence has been collected for a period of time.		
98	Solution should provide information on the threat present on the customer‘s network (i.e. Bank’s network) (threat details, threat intent, researcher notes, crime ware used, local communication activity, etc.).		
99	Solution should be able to pick up and reconstruct suspicious files via a passive interface and make the files accessible to administrators with rights to download malicious files.		
100	Solution should allow customer access to suspicious and malicious files so that they can download them, process them themselves, or submit to their AV vendor for signature creation.		
101	Solution should allow for categorization of devices along with level of importance‘ of those devices should they be infected, with the following priority:- Critical, High, Medium, Low		
102	Solution must provide infection forensics to enable incident responders to validate findings and adapt security policy (connection attempt counts, connection attempt success, bytes in, bytes out, full packet captures, suspicious file static and dynamic analysis, Forensic Metadata and Infection Forensics)		
103	Solution should be able to track if remediation efforts have been effective by continually monitoring the network behaviours of an asset and keeping a threat history (including all evidence).		
106	Solution should be able to perform DNS redirection for malicious DNS queries, to prohibit infections from communicating with cyber criminals.		
107	Solution should be able to perform TCP RSTs for individual communication sessions with C&Cs to protect against the loss of data.		
108	Solution should support the ability to forward logs		
109	Solution should report infection alerts on a real time basis via email.		
110	Solution should support device alerting for the health of the solution via the industry-standard simple network Management protocol (SNMP v3) traps and alerts.		
111	Solution should provide a high performance architecture with comprehensive layered malware protection including Antivirus, Threat Intelligence, and Gateway Anti Malware and advance sandboxing all from a single OEM and should not be a combination from different OEM’s		
112	The solution should have built-in SSL decryption Engine (or integration with SSL offloader to be provided by bidder) for Inbound SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured http channel without need to have additional appliances		
113	The solution should provide protection for web application server against advance attacks such as SQL Injections not on signature basis only but also on Heuristic basis also.		
114	The solution should have the ability to block connection to or from outside based on the reputation of the IP address that is trying to communicate with the network using global threat intelligence		

115	The solution should support provide advanced botnet protection using heuristic detection methods		
116	The Solution should support atleast 10 multiple simultaneous VM images for target specific Sandboxing to identify malware.		
117	The solution should provide the ability to upload and analyze objects through a collection of custom virtual machines rather than a generic image.		
118	The solution should have the ability to unpack the code and remove any obfuscation to identify the original executable code.		
119	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.		
120	The solution should provide the ability to upload gold image and analyze threats under conditions of actual host environment.		
121	The solution should provide real-time intelligence about the behavior of the suspect code without requiring any signatures or updates from the vendor		
122	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the Bank's network.		
123	The Anti-APT Solution should have minimum 50 Sandboxes and should be able to handle at least 25000 files in a day		
124	The solution should support open web Services API for 3rd party or scripting integration		

Deception Solution

SN	Technical Specification	Compliance (Yes/No)	Remarks, if any
1	The solution must have the ability to visually replay past events on an interactive fluid dashboard that show all decoy elements and attacker details.		
2	Solution must allow visual dissection of the PCAP traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter.		
3	Solution must provide built in signature detection for 'known bad' events and must be updated with the latest emerging threat signatures.		
4	Solution must use a numeric risk score for each attacker based on dynamic analysis of attacker behaviour. Solution should not just use basic critical / high / medium / low buckets.		
5	The system must have the ability to save and share custom views filtered based on time and any event metadata for analysing specific events. Results of saved queries must be exportable.		
6	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker / APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.		
7	The solution should have a central management console to manage the deployment and event notifications. All other components should be controlled and configured through the central management console only.		

8	Both physical and virtual instances that can each support minimum 50 VLANs and minimum 250 network decoys per appliance.		
9	Decoys created should be added as computer objects to the real Active Directory domain and should not use a domain trust relationship between a dummy Active Directory and the real Active Directory domain that hackers can easily discover.		
10	The solution should have capabilities to scan the surrounding environment, and automatically deploy authentic deception that mimic not only the hostnames of the surrounding systems but MAC addresses and services as well. The solution must be able to choose the ratio between blend-in and stand-out decoys.		
11	Ability to agentlessly embed lures on real endpoints in the form of unique dummy credentials that lead attackers on to decoy systems		
12	Deception platform must be capable of creating file decoys that are deployed on real systems and agentlessly trigger alerts not only when opened but also when copied, modified and deleted		
13	The solution should have the ability to capture commands executed for hi-interaction SSH connections on Linux decoys without any instrumentation processes or agents running within the decoys.		
14	Decoy services like SSH, HTTP / HTTPS, FTP, SMB, MySQL, telnet should be individually unique services and not just a few VMs offering the same service on multiple IP addresses		
15	The solution should be able to deploy built in application decoys that look like webmail portals, vpn login portals, network printer, PIM login, HRMS etc.		
16	Decoy web-applications should include the ability to easily upload templates for high-interaction (login / browsing of the decoy application).		
17	All Windows high interaction activity should be logged, not just code execution attempts. High-interaction should not involve transfer of malicious code to a separate analysis VM, but should provide full interactive access to the attacker.		
18	Solution should include high-interaction Windows decoys that are accessible over the following channels: WMI, RDP, WinRM, RPC-DCOM.		
19	The solution should have the ability to record the screen in a video (NOT screenshots) and must also capture keystrokes and mouse movements for hi-interaction remote desktop connections on Windows decoys and provide a downloadable video replay with keystroke capture of the attacker's activity in the decoy.		
20	The solution must support geolocation of external threats.		
21	Deception platform should automatically fill network decoys with realistic auto-generated enticing content containing folders and files pertaining to specific business verticals like Finance, Legal, HR, IT etc. The number of folders and files to generate and the file creation dates (oldest to newest) should be configurable. The files generated should be a combination of terms relating to specific verticals as well as pre-configured keywords related to the organisation.		
22	The solution should be able to create 250 network decoys (windows and Linux) from a single appliance with individual NETBIOS hostnames per decoy IP.		
23	The solution should have the ability to detect network scans in all VLANs in the enterprise network including remote offices without the need for any complex network changes like GRE tunnels or additional		

	virtual appliances in each branch		
24	The solution must support deep protocol inspection of network traffic such as DCE/RPC / SSL-JA3 for detection of exploits.		
25	The solution should be able to create spear-phishing decoys to detect targeted spear phishing attempts.		
26	For authenticity, Linux high-interaction decoys should be one-to-one (the solution should not re-use of a few internal VMs configured with multiple IPs to show multiple decoys).		
27	The deception appliance should be able to create decoys that have only one network interface. This should be applicable even when 50 or more such decoys are deployed from an appliance.		
28	Besides email alerts, the solution must have the built in ability for real-time voice phone calls and SMS alerts based on preset or custom notification rules		
29	The solution should have a built in incident response capability that allows interactive forensics of the attacking source system, not just a snapshot memory dump.		
30	The solution should have an inbuilt feature to allow automatic isolation of of an attacking source system based on preset or custom rules. This should be possible without relying on integrations to external systems.		
31	When an event occurs, the solution should have built in orchestration to take specific actions based on preset or user specified rules that can be specified on any event meta-data. The rule engine should support multiple boolean and logical conditions to appropriately orchestrate the response.		
32	For security, the base operating platform (host operating platform on which the decoys run) of the deception appliance should be different from the decoy OS's		
33	For security, the solution must have a high-security, sandboxed hypervisor and use nested virtualisation where the decoys run inside the sandboxed hypervisor within the appliance.		
34	The solution should proive a GUI for user to control the applications		
35	The system should detect all types of attack vectors including but not limited to pre attack reconnaissance, spear phishing , zero- day attacks, privilege escalation, lateral movement, data theft and malware		
36	The solution must include integrated sandboxing capabilities for detonating malwares and files that are being used as part of the attack		
37	Solution should provide deep visibility into the Vlans in the form of assests, services, os, etc. and must record and alert incase of any new endpoint connects to the vlan.		
38	The solution should provide a sinkhole capability to redirect the attacker and allow the attack to develop and progress outside production environment		
39	The solution must have an API integration with the existing security and network products of the bank for automated sharing of attack information.		
40	The solution should be able to assign multiple IP addresses across subnets to decoys through DHCP or static IP addressing		
41	Solution should support ability to deploy a Windows Active Directory server as a target instance or integrate the decoys and deceptive		

	users with the production AD. Should have the ability to create deception in the Active Directory (AD), without using the real AD instead of a dummy AD / trust relationship.		
42	Solution should be able to provide web-application decoys or mobile application decoy to guard against business logic attacks.		
43	Solution should automatically detect scanning and L2 attacks such as ARP flood and IP scan etc.		
44	The solution should support deceptive objects (breadcrumbs) on production endpoints centrally from the management console without relying on 3rd party tools		
45	The deceptive objects (breadcrumbs) should be dynamic in nature and based on learning by the platform , the objects should refresh with enticing false credentials		
46	Solution should provide fully liscensed real OS decoys and not emulated services. Should support the current version OS running in th bank environment		
47	Solution must support automatic and adaptive decoy deployment and VLAN discovery without using any template for deployment.		
48	Solution should support import of custom OS (golden image) as target instances and provide capability to license the OS and installed applications		
49	The solution should be capable of mimicking other devices like printers, switches, routers, Voice over IP phones and Video Cameras		
50	Solution should provide maintainance mode wherein decoys of a particular VLAN can be switched off during maintainance of the VLAN		
51	The solution should integrate with existing patch management solution of the bank to keep the decoys in sync with the patch level of devices in production environment		
52	Solution should support synchronization with NTP servers and push the same on decoys		
53	Solution should support download of all endpoint deceptive object infromation in CSV file		
54	The solution should support creation of unlimited number of decoys and the number of decoys per VLAN should be controlable from the management console		
55	Solution should be capable to integrate with firewall on API and isolate the endpoints that are being used for attack or botnet using automated rules.		
56	The solution should not only depend on static signatures and heuristics to identify attacks		
57	The decoys should automatically be refreshed to create access timestamp on the decoys		
58	Solution should provide ability to upload suspected samples from platform UI to inbuilt sandbox for malware analysis		
59	Solution should provide ability to forward emails to sandboxing funcionality for email/malware analysis		
60	Solution should allow submitting sample hash or sample file to Virus Total to detect known malware		
61	The solution should include the capability to automatically triage and extract forensics information from infected / compromised assets		
62	Web application decoys should be able to provide full licensed application deceptions of solutions currently deployed in bank		
63	The solution should be able to replay the attack carried out on the		

	decoy for further analysis		
64	The solution must support the detection of the Man in the Middle in DC & remote locations. Attack for the following protocols: NBNS, LLMNR, MDNS, ARP, DHCP		
65	The solution should support a dashboard of all endpoints where breadcrumbs are installed together with details on what was installed and where.		
66	The solution must support path discovery and provide topographical network map for lateral movements to critical assets.		
67	Solution must include all system, browser and application credentials and must maintain current timestamps and must be hidden from normal users.		
68	Solution should have API based integration with bank's existing security solutions like Firewalls, NAC , SIEM etc.. To automatically take an action (Quarantine or block) the infected machine or IP.		
69	The solution should support sending Darknet IP traffic to the platform. Should be able to create unused IP's in production subnets and dark networks on routers and forward traffic to these IP's to deceptive VM's for engagement.		
70	Solution should be able to spin up or create an automatic decoy as per the request seen from the attacker.		
71	System should be able to detect and track stolen credentials by integrating with SIEM on API's		
72	Solution should provide fully licensed real OS decoys and not emulated services. Should support Windows and Linux operating systems (Red hat Linux, Ubuntu, Centos) .		
73	The solution should support the randomization of false credentials.		
74	The solution should have the capability to deploy clients for endpoints spread across branches all over India, through a central tool or the bidder has to arrange for the same through visit at these locations.		

Date:_____
Place:_____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Seal of Company

PERFORMA FOR INDICATIVE COMMERCIAL OFFER

RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

Table-A: Network Anti- Advanced Persistent Threat (N/w-Anti-APT)

Sr.No.	Mandatory Items	Unit Cost (a)	Multiplication Factor (b)	Total Cost (c=a*b)
1.	Total Hardware Cost		HA at both DC & DR	
2.	Total Software cost including all required licenses		**1**	
3.	End-to-End Implementation Cost (both for DC & DR)		**1**	
4.	AMC of hardware per year (range Minimum 5%-Maximum 10% of Sr.No.1)		**2**	
5.	ATS for software per year (range Minimum 10%-Maximum 20% of Sr.No.2)		**2**	
6	Additional OTS Cost of L2 resource (man month charges)(as and when required)*		**6**	
	Total of Table A (1+2+3+4+5+6)			

*to be deployed at DC & DRS

Table B-Deception Solution

Sr.No.	Mandatory Items	Unit Cost (a)	Multiplication Factor (b)	Total Cost (c=a*b)
1.	Total Hardware Cost		HA at both DC & DR	
2.a.	License cost for DC VLANs		**150**	
b.	License cost for DR VLANs		**100**	
c.	Any other software or licenses required		**1**	
d.	Total of software cost including all required licenses **(a+b+c)**			
3.	License cost for Endpoints		**20000**	
4.	End-to-End Implementation Cost (both for DC & DR)		**1**	
5.	AMC of hardware per year (range Minimum 5%-Maximum 10% of Sr.No.1)		**2**	
6.	ATS for DC-DR License per year (range Minimum 10%-Maximum 20% of Sr.No.2d)		**2**	

7.	ATS for endpoint License per year (range Minimum 10%-Maximum 20% of Sr.No.3)		**2**	
8.	Additional OTS Cost of L2 resource (man month charges)(as and when required)*		**5**	
	Total of Table A (1+2d+3+4+5+6+7+8)			

*to be deployed at DC & DRS

Table C: Total cost of Both the solutions

	Items	**Total Cost**
1	**Total of Table A**	
2	**Total of Table B**	
	Grand Total	

NOTES:

1. The rates quoted in commercial bid should be inclusive of all taxes except GST. However, GST shall be paid to the bidder on actual basis at the rate applicable. The rate of applicable GST should be informed and charged separately in the invoice generated for supply of the product.
2. Any column left blank by the bidder will result in disqualification of the bid.
3. Price of hardware & software quoted should be inclusive of 3 years warranty.
4. AMC/ATS will be applicable after expiry of warranty period of three years.
5. ATS/AMC should be quoted in the specified range only. If quoted lower or beyond the specified range, it will automatically be recalculated. For eg. In case AMC is quoted lower than 5% it will be recalculated at 5% and if quoted higher than 10% it will be recalculated at 10%.
6. L1 cost will be decided as per total of Table C, after Reverse Auction is conducted as per Clause 25 of Instruction to Bidder.
7. Bank may place Orders for any item as and when required during the entire contract period at the unit rates finalized after Reverse Auction. Bank is not bound to place any minimum order. The quantity will also be as per requirement.
8. The multiplication factor as mentioned in above tables is only indicative and for the purpose of deriving the Total Cost for determining the L1 bidder. The actual quantity of any item ordered may vary according to the requirement of the Bank. In addition to the initial Order placed, Bank may place subsequent orders for any item, if required, at any time during the contract period of 5 years, at the unit rate finalized after Reverse Auction.
9. Bank is not bound to place any minimum order for any item.

Date: _____
Place: _____
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-XIV

PERFORMA FOR THE BANK GUARANTEE FOR EARNEST MONEY DEPOSIT

To be stamped in accordance with stamp act)

Ref: Bank Guarantee # Date
Punjab National Bank
Information Technology Division
5, Sansad Marg
New Delhi 110001

Dear Sir,

In accordance with your bid reference no. _____ Dated _____ M/s_____having its registered office at _____herein after Called 'bidder') wish to participate in the said bid for RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions.

An irrevocable Bank Guarantee (issued by a nationalized / scheduled commercial Bank) against Earnest Money Deposit amounting to Rs._____ Rupees (in words_____) valid up to is required to be submitted by the bidder, as a condition for participation in the said bid, which amount is liable to be forfeited on happening of any contingencies mentioned in the bid document.

M/s_____ having its registered office at _____ has undertaken in pursuance of their offer to Punjab National Bank (hereinafter called as the beneficiary) dated _____ has expressed its intention to participate in the said bid and in terms thereof has approached us and requested us_____ (Name of Bank)_____ (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs_____/- Rupees (in words_____) valid up to.

We, the _____ (Name of Bank)_____ (Address of Bank) having our Head office at _____ therefore Guarantee and undertake to pay immediately on first written demand by Punjab National Bank, the amount Rs._____ Rupees (in words_____) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the bidder.

This guarantee shall be irrevocable and shall remain valid up to . If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from _____, on whose behalf guarantee is issued.
"Not withstanding anything contained herein above
Our liability under this Bank guarantee shall not exceed Rs _____ Rupees (in words_____).

This Bank guarantee shall be valid up to. We are liable to pay the guaranteed amount or any part thereof under this Bank guarantee only if you serve upon us a written claim or demand, on or before hours (Indian Standard Time) where after it ceases to be in effect in all respects whether or not the original Bank guarantee is returned to us."

In witness whereof the Bank, through its authorized officer has set its hand stamped on this _____ Day of _____2018 at _____

Date: _____
Place: _____

Signature of Authorized Signatory

Name of Signatory:
Designation:
Seal of Company

PERFORMA FOR INTEGRITY PACT

To,
The Asstt. General Manager,
IT Procurement Department, HO: ITD
Punjab National Bank,
……
New Delhi

Subject: Submission of Tender for the work……

Dear Sir,

I/We acknowledge that Punjab National Bank is committed to follow the principle of transparency equity and competitiveness as enumerated in the Integrity Agreement enclosed with the tender/bid document.

I/We agree that the Notice Inviting Tender (NIT) is an invitation to offer made on the condition that I/We will sign the enclosed integrity Agreement, which is an integral part of tender documents, failing which I/We will stand disqualified from the tendering process. I/We acknowledge that THE MAKING OF THE BID SHALL BE REGARDED AS AN UNCONDITIONAL AND ABSOLUTE ACCEPTANCE of this condition of the NIT.

I/We confirm acceptance and compliance with the Integrity Agreement in letter and spirit and further agree that execution of the said Integrity Agreement shall be separate and distinct from the main contract, which will come into existence when tender/bid is finally accepted by Punjab National Bank. I/We acknowledge and accept the duration of the Integrity Agreement, which shall be in the line with Article 6 of the enclosed Integrity Agreement.

I/We acknowledge that in the event of my/our failure to sign and accept the Integrity Agreement, while submitting the tender/bid, Punjab National Bank shall have unqualified, absolute and unfettered right to disqualify the tenderer/bidder and reject the tender/bid is accordance with terms and conditions of the tender/bid.

Yours faithfully

(Duly authorized signatory of the Bidder)

To be signed by the bidder and same signatory competent / authorized to sign the relevant contract on behalf of Punjab National Bank.

INTEGRITY AGREEMENT

This Integrity Agreement is made at ..... on this .....day of .....2019.

BETWEEN

Punjab National Bank is a Bank constituted under The Banking Companies (Acquisition & Transfer of Under-takings) Act 1970, having its Head Office at Sector 10, Dwarka, New Delhi-110075 and inter-alia a Branch Office/ Circle Office at _____ (Hereinafter referred as the Principal/Owner', which expression shall unless repugnant to the meaning or context hereof include its successors and assigns)

AND……..... (Name and Address of the Individual/firm/Company) Through..... .... Details of duly authorized signatory) (Hereinafter referred to as the "Bidder/Contractor" and which expression shall unless repugnant to the meaning or context here of include its successors and permitted assigns)
Preamble

WHEREAS the Principal / Owner has floated the Tender for (……..Name of Work……..) (hereinafter referred to as "Tender/Bid") and intends to award, under laid down organizational procedure, contract for …… …… ……hereinafter referred to as the "Contract".

AND WHEREAS the Principal/Owner values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relation with its Bidder(s) and Contractor(s). AND WHEREAS to meet the purpose aforesaid both the parties have agreed to enter into this Integrity Agreement (hereinafter referred to as "Integrity Pact" or "Pact"), the terms and conditions of which shall also be read as integral part and parcel of the Tender/Bid documents and Contract between the parties.

NOW, THEREFORE, in consideration of mutual covenants contained in this Pact, the parties hereby agree as follows and this Pact witnesses as under:

Article 1: Commitment of the Principal/Owner

1) The Principal/Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:

(a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender, or the execution of the Contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

(b) The Principal/Owner will, during the Tender process, treat all Bidder(s) with equity and reason. The Principal/Owner will, in particular, before and during the Tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the Tender process or the Contract execution.

(c) The Principal/Owner shall Endeavour to exclude from the Tender process any person, whose conduct in the past has been of biased nature.

2) If any information comes to the notice of the Principal/owner on the conduct of any of its employees which is a criminal offence under the Indian Penal code (IPC)/Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there be a substantive suspicion in this regard, the Principal/Owner will inform the Asstt. General Manager Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

Article 2: Commitment of the Bidder(s)/Contractor(s)

1) It is required that each Bidder/Contractor (including their respective officers, employees and agents) adhere to the highest ethical standards, and forthwith report the Principal/Owner about all suspected fraudulent act or corruption or Coercion or Collusion of any person connected with the tender process which it has knowledge or becomes

aware any time, during the tendering process and throughout the negotiation or award of a contract.

2) The Bidder/Contractor commits himself/itself to take all measures necessary to prevent corruption. He/it commits himself/itself to observe the following principles during his/its participation in the Tender process and during execution of the Contract:
a) The Bidder/Contractor shall not, directly or through any other person or firm, offer, promise or give to any of the Principal/Owner's employees involved in the Tender process or execution of the Contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the Tender process or during the execution of the Contract.

b) The Bidder/Contractor shall not enter with other Bidder(s) into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to cartelize in the bidding process.

c) The Bidder/Contractor will not commit any offence under the relevant IPC/PC Act. Further the Bidder/Contract will not use improperly, (for the purpose of competition or personal gain), or pass on to others, any information or documents provided by the Principal/Owner as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted Electronically.

3. The Bidder/Contractor of foreign origin shall disclose the names and addresses of agents/ representatives in India, if any. Similarly Bidder/Contractor of Indian Nationality shall disclose names and addresses of foreign agents/representatives, if any. Either the Indian agent on behalf of the foreign principal or the foreign principal directly could bid in a tender but not both. Further, in cases where an agent participate in a tender on behalf of one manufacturer, he shall not be allowed to quote on behalf of another manufacturer along with the first manufacturer in a subsequent/parallel tender for the same item.

4. The Bidder/Contractor will, when presenting his/its bid, disclose any and all payments he/it has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the Contract.

5. The Bidder/Contractor will not instigate third persons to commit offences outlined above or be an accessory to such offences.

6. The Bidder/Contractor will not, directly or through any other person or firm indulge in fraudulent practice means a willful misrepresentation or omission of facts or submission of fake/forged documents in order to induce public official to act in reliance thereof, with the purpose of obtaining unjust advantage by or causing damage to justified interest of others and/or to influence the procurement process to the detriment to the interests of Principal/Owner.

7. The Bidder/Contractor will not, directly or through any other person or firm use Coercive Practices against principal/owner and/or other bidder(s)/contractor(s). Coercie practices mean the act of obtaining something, compelling an action or influencing a decision through intimidation, threat or the use of force directly or indirectly, where potential or actual injury may befall upon a person, his/ her reputation or property to influence their participation in the tendering process.

Article 3: Consequences of Breach

Without prejudice to any rights that may be available to the Principal/Owner under law or the Contract or its established policies and laid down procedures, the Principal/Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder(s)/Contractor(s) and the Bidder/ Contractor accepts and undertakes to respect and uphold the Principal/Owner's absolute right:

1) If the Bidder/Contractor, either before award or during execution of Contract has committed a transgression through a violation of Article 2 above or in any other form, such as to put his reliability or credibility in question, the Principal/Owner at its discretion, is entitled to disqualify the Bidder/Contractor from the Tender process or terminate/determine the Contract, if already executed or exclude the Bidder/Contractor from future contract award processes after giving 14 days' notice to the contractor. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by the Principal/Owner. Such exclusion may be forever or for a limited period as decided by the Principal/Owner.

2) Forfeiture of EMD/Performance Guarantee/Security Deposit: If the Principal/Owner has disqualified the Bidder(s) from the Tender process prior to the award of the Contract or terminated/determined the Contract or has accrued the right to terminate/determine the Contract according to Article 3(1), the Principal/Owner apart from exercising any legal rights that may have accrued to the Principal/Owner, may in its considered opinion forfeit the entire amount of Earnest Money Deposit, Performance Guarantee and Security Deposit of the Bidder/Contractor.

3) Criminal Liability: If any act/omission or conduct of a Bidder or contractor conduct of a Bidder or Contractor, or of an employee or a representative or an associate of a Bidder or Contractor which constitutes corruption within the meaning of IPC/PC Act brought to the notice of the Principal/Owner, or if the Principal/ Owner has substantive suspicion in this regard, the Principal/Owner shall be at liberty to inform the same to law enforcing agencies for further investigation.

Article 4: Previous Transgression

(i) The Bidder declares that no previous transgressions occurred in the last 5 years with any other Company in any country confirming to the anticorruption approach or with Central Government or State Government or any other Central/State Public Sector Enterprises in India that could justify his exclusion from the Tender process.

(ii) If the Bidder makes incorrect statement on this subject, he can be disqualified from the Tender process or the contract, if already awarded, can be terminated for such reason. Principal/owner will be entitled to exclude the contractor from future tender/contract award processes for a period not exceeding three years.

(iii) Without prejudice to any other legal rights or remedies available to the principal under the relevant clauses of the tender document.

Article 5: Equal Treatment of all Bidders/Contractors/Subcontractors

2) The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder/Contractor shall be responsible for any violation(s) of the principles laid down in this agreement/Pact by any of its Subcontractors/ sub-vendors.

3) The Principal/Owner will enter into Pacts on identical terms as this one with all Bidders and Contractors.

4) The Principal/Owner will disqualify Bidders, who do not submit, the duly signed

Pact between the Principal/Owner and the bidder, along with the Tender or violate its provisions at any stage of the Tender process, from the Tender process.

Article 6- Duration of the Pact

This Pact begins when both the parties have legally signed it. It expires for the Contractor/ Vendor 12 months after the completion of work under the contract or till the continuation of defect liability period, till the Contract has been awarded. If any claim is made/lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Pacts as specified above, unless it is discharged/ determined by the Competent Authority, Punjab National Bank.

Article 7-Independent External Monitor (IEM)

1. The Principal/Owner has appointed competent and credible Independent External Monitor(s) (IEM) Sh._____ & Sh._____for this Pact in consultation with the Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to MD& CEO, Punjab National Bank.

3. The Bidder/Contractor accepts that the IEM has the right to access, without restriction, to all Project documentation of the Principal/Owner including that provided by the Contractor. The Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-Contractor's project documentation. The IEM is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality.

4. In case of tenders having estimated value exceeding Rs 60 lakhs, the Principal/Owner will provide to the IEM sufficient information about all the meetings among the parties related to the Project and shall keep the IEM apprised of all the developments in the Tender Process.

5. As soon as the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal/Owner and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. However, beyond this, the IEM has no right to demand from the parties that they act in a specific manner, and/or refrain from action or tolerate action.

6) The IEM shall submit a written report to the MD & CEO, of the Principal/Owner within 6 to 8 weeks from the date of reference or intimation to him by the Principal/Owner and, should the occasion arise, submit proposals for correcting problematic situations.

7) The word "IEM" would include both singular and plural.

8) IEMs will not use or pass on any information or document provided to it regarding plans, technical proposals and business details for the purpose of competition or personal gains etc.

Article 8- Other Provisions

1. This Pact is subject to Indian Law, place of performance and jurisdiction is place where office of the Principal/Owner, who has floated the Tender, is located.

2. Changes and supplements need to be made in writing.

3. If the Contractor is a partnership or a consortium, this Pact must be signed by all the partners or consortium members. In case of a Company, the Pact must be signed by a representative duly authorized by board resolution.

4. Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intensions.

5. It is agreed term and condition that any dispute or difference arising between the parties with regard to the terms of this Integrity Agreement / Pact, any action taken by the Owner/Principal in accordance with this Integrity Agreement/ Pact or interpretation thereof shall not be subject to arbitration.

Article 9- LEGAL AND PRIOR RIGHTS

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and/or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agree that this Integrity Pact will have precedence over the Tender/Contact documents with regard any of the provisions covered under this Integrity Pact. IN WITNESS WHEREOF the parties have signed and executed this Integrity Pact at the place and date first above mentioned in the presence of following witnesses:

..... (For and on behalf of Principal/Owner)

..... (For and on behalf of Bidder/Contractor)

WITNESSES:
1. ..... (Signature, name and address)

2. ..... (Signature, name and address)

Place:
Dated:

ANNEXURE - XVI

CHECKLIST

Sl. No.	Particulars	Submitted (Yes/No)	Page No
1.	Proof of RFP Cost		
2.	Proof of EMD		
3.	Terms and Conditions (Annexure-I)		
4.	Undertaking By The Bidder (Annexure-II)		
5.	Compliance To Eligibility Criteria (Annexure III)		
6.	Bidders Information (Annexure-IV)		
7.	Compliance Statement (Annexure-V)		
8.	Litigation Certificate (Annexure – VII)		
9.	Undertaking For Non- Blacklisted(Annexure – VIII)		
10.	Turnover Certificate by CA(Annexure-IX)		
11.	Manufacturer's Authorization Form (MAF) (Annexure-X)		
12.	Undertaking for being the OEM of the offered Application(Annexure-XI)		
13.	Technical Specifications (Annexure – XII)		
14.	Certificate of Incorporation		
15.	Complete Bill of Material (BOM) (Both hardware & Software)		
16.	Undertaking of Information Security		
17.	Audited Balance Sheets & Profit & Loss Statements		
18.	Integrity Pact (Annexure – XV)		
19.	Power of Attorney and Copy of Board Resolution		