Central Bank of India

Tender Reference No.CO:DIT:PUR:2016-17:226

Request for Proposal (RFP)

For

Appointment of Security Consultant

For

Implementing Cyber Security Framework in Bank

Central Bank of India invite bids for appointment of Security Consultant for Implementing Cyber Security Framework in the Bank.

Important information regarding Bid submission

Tender Reference No.	CO:DIT:PUR:2016-17:226
Price of Tender copy/ Application money	Rs.5,000/-
Earnest Money Deposit (EMD)	Rs. 50,000/-
Date of commencement of sale of RFP	23.08.2016
Submission of Queries, Error & Omission in respect of RFP	On or before 26.08.2016
Date , Time & Venue of Prebid meeting	30.08.2016 at 3.00 pm Department of Information Technology, Central Office, Central Bank Of India Central Bank Building, 1st Floor, DIT, Sector 11, CBD Belapur, Navi Mumbai - 400614
Last date and time for receipt Bids	14.09.2016 upto 3.00 pm
Date and time of opening Technical bid	14.09.2016 at 3.30 pm
Place of submission of Bids	Asst. General Manager -IT, Central office, Central Bank Of India Central Bank Building, 1st Floor, DIT, Sector 11, CBD Belapur, Navi Mumbai - 400614
Address for communication	Same as above
Place of opening bids	Same as above
Contact numbers	022 - 6712 3669/3583 / 3552
E-mail address	ciso@centralbank.co.in cminfosec@centralbank.co.in sminfosec@centralbank.co.in smitpurchase@centralbank.co.in
Fax numbers	022-27576378
Web site	www.centralbankofindia.co.in

Bidders are requested to submit their Technical and Commercial offers in two separate sealed envelopes super scribing "Bid for Appointment of Security Consultant for Implementing Cyber Security Framework TENDER NO. 226 . (Technical Bid)" and "Bid for appointment of Security

Consultant for Implementing Cyber Security Framework in the Bank TENDER NO. 226 (Commercial Bid)", respectively.

The copy of tender document may be down loaded from Bank's website www.centralbankofindia.co.in and cost of the same be remitted on or before the pre-bid meeting.

CONTENTS

1.	ABOUT THE BANK	6
2.	INTRODUCTION AND DISCLAIMER	6
3.	INFORMATION PROVIDED	6
4.	FOR RESPONDENT ONLY	7
5.	DISCLAIMER	7
6.	COSTS BORNE BY RESPONDENTS	7
7.	NO LEGAL RELATIONSHIP	7
8.	RECIPIENT OBLIGATION TO INFORM ITSELF	7
9.	EVALUATION OF OFFERS	7
10.	ERRORS AND OMISSIONS	7
11.	PREBID MEETING	8
12	ACCEPTANCE OF TERMS	8
13.	LODGMENT OF RFP RESPONSE	8
14	NOTIFICATION	8
15.	DISQUALIFICATION	9
16.	PROCESS	9
17.	CURRENT RFP OBJECTIVES	9

18. BIDDER ELIGIBILITY CRITERIA 13

19. EARNEST MONEY DEPOSIT 14

20. APPLICATION MONEY 14

21. SUBMISSION OF BIDS (PLEASE REFER TO PARA 12) 14

22. GENERAL TERMS AND CONDITIONS 16

23. BID EVALUATION CRITERIA 22

24. ANNEXURES 25

1. About the Bank

Central Bank of India herein after referred to as the "Bank", established in 1911, was nationalized in the year 1969 and today is a leading public sector bank listed in BSE/NSE.

The organizational structure of the Bank consists of four tiers viz., Central Office (CO), Zonal Offices (ZO), Regional Offices (RO) and Branches. CO, consisting of various functional departments deals with mainly policy formulation, setting of targets and monitoring of performance. The Bank has set up 13 Zonal Offices to exercise immediate supervision and control over the 59 Regional Offices, which in turn supervise the branches under their jurisdiction. The Bank has a network of 4700 plus offices, spread across the length and breadth of the country with presence in all the States and Union Territories. The Bank has also established its Wide Area Network at 4700 plus locations all over India covering administrative and branch offices and is planning to enlarge it during the current year.

The Bank also has specialized branches catering to the specific needs of Retail customers, Industrial units, corporate clients, Forex dealers, Exporters and Importers, Small Scale Industries and Agricultural sector. The Bank has sponsorship in 3 Regional Rural Banks (RRB).

2. Introduction and Disclaimer

This Request for Proposal document ("RFP") has been prepared solely to enable Central Bank of India ("Bank") in defining the requirements for appointment of Security Consultant for Implementing Cyber Security Framework in the Bank.

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the services.

3. Information Provided

The RFP document contains statements derived from information that is believed to be reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services.

Neither the Bank nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document.

Neither the Bank nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification or due diligence exercise in relation to the contents of any part of the RFP document.

4. For Respondent Only

The RFP document is intended solely for the information of the party to whom it is issued ("the Recipient" or "the Respondent") and no other person or Organization.

5. Disclaimer

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

6. Costs Borne by Respondents

All costs and expenses incurred by Recipients / Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by Bank, will be borne entirely and exclusively by the Recipient / Respondent.

7. No Legal Relationship

No binding legal relationship will exist between any of the Recipients / Respondents and Bank until execution of a contractual agreement.

8. Recipient Obligation to Inform Itself

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

9. Evaluation of Offers

Each Recipient acknowledges and accepts that Bank may, in its absolute discretion, apply whatever criteria it deems appropriate in the selection of Organization's, not limited to those selection criteria set out in this RFP document.

The RFP document will not be construed as any contract or arrangement which may result from the issue of this RFP document or any investigation or review carried out by a Recipient. The Recipient acknowledges by submitting its response to this RFP document that it has not relied on any information, representation, or warranty given in this RFP document.

10. Errors and Omissions

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

11. Pre-bid Meeting

Queries, error & omission in respect of RFP, to be submitted on or before the date mentioned above. Document fee of Rs. 5000/- has to be submitted on or before the pre-bid meeting to attend the same. Those who has submitted Document fee of Rs. 5000/-, only will be allowed to participate in the pre-bid meeting. However, Bank may clarify the queries of those who choose not to attend the pre-bid meeting also.

12. Acceptance of Terms

A Recipient will, by responding to Bank RFP, be deemed to have accepted all the terms and conditions as stated in this RFP.

13. Lodgment of RFP Response

13.a. RFP Closing Date

RFP Response shall be received within the stipulated date/time by the officials at the address mentioned above.

One (1) electronic copy of the technical offer in CD ROM should also be submitted at the time of offer submission by the bidders.

13.b. Requests for Information

All questions relating to the RFP, technical or otherwise, must be in writing/email only to the Nominated Point of Contact.

The Bank will clarify only those queries received within the prescribed date and time mentioned above. However, the Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent's response.

If the Bank in its absolute discretion deems that the originator of the question will gain an advantage by a response to a question, then Bank reserves the right to communicate such response to all Respondents.

Bank may in its absolute discretion engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify a response.

14. Notification

Bank will notify the Respondents in writing/email as soon as practicable about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been

accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

15. Disqualification

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

16. Process

Selection of a successful Service Provider will involve a five (5) stage approach.

a. Issue of RFP document.
b. Receipt of RFP document.
c. Opening of the RFP.
d. Technical & Commercial Evaluation of offers.
e. Finalization of successful bidder.

1. Due to unforeseen reasons, if the RFP closing date happens to be a Bank Holiday, the closing date for submission of RFP should be automatically extended to next immediate working date.

2. Authorization letter should be issued by the bidders company to the representative or attending the meeting is required.

3. All the shortlisted intending bidders have to make a presentation before the panel of Bank Officials.

17. Current RFP Objectives

17.a. Project Objective

The Bank wishes to appoint competent Consultant for implementing Cyber Security Framework in the Bank. The broad scope of work for the appointed security consultant would be to assist in complete implementation of cyber security framework in the bank in line with RBI circular no. RBI/2015-16/418 dated 02-Jun-2016.

In view of the recent cyber-attacks in financial sectors, Reserve Bank of India has published guidelines on Cyber Security frameworks for Bank's vide circular no. RBI/2015-16/418 DBS.CO.CSITE/BC.11/33.01.001/2015-16 dated 02-Jun-2016. The Bank including its RRBs (Regional Rural Banks sponsored by the Bank) has implemented its centralized systems at Data Centre and DR site and it intends to strengthen its Cyber attack detection and response mechanism so that in case of any indicator of compromise, Bank can detect the same and respond before the actual damage takes place. Based on the contents of the RFP, the selected Bidder shall be required to independently arrive at approach and methodology, based on RBI Cyber Security Framework, RBI Gopal Krishnan Committee Report recommendations and

other International best practices. The approach and methodology will be approved by the Bank.

The Bank expressly stipulates that the Consultant's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire assignment and that delivery of the deliverables and the services in connection therewith are only a part of the assignment. The selected Bidder shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment at no additional cost to the Bank. The selected Bidder will be responsible for carrying out following major tasks :

1. Performing Gap Assessment of Bank's existing infrastructure/security measures and assisting in remedial/improvement measures to comply with respect to RBI Guidelines dated 02-Jun-2016.

2. Drafting Cyber Security Policy as per international best practices.

3. Formulating Cyber Crisis Management Plan.

4. Formulating Digital Evidence Policy

5. Assisting in implementing Cyber-Security Operation Centre (C-SOC) through formal tender process

6. Implementation of effective Incident Management Response Structure and Process

7. Review and updation of existing Minimum Baseline Security Documents to include cyber security aspects.

Bank may, at its full discretion, choose to avail of the services for all services or part thereof. Such decision may be advised in course of the project.

17.b. Consultancy Project Scope

The Bank expressly stipulates that the Security Consultant selection under this RFP is on the understanding that this RFP contains only the principal provisions for the aforesaid activities.

The primary focus of the scope is to strengthen cyber defense and response mechanism of the Bank. The scope will cover all the threat vectors whether known or unknown, identify gaps in its defense and strengthen its defense against such attacks. Following outlines the scope of work to be carried out by the selected Bidder.

1. Performing Gap Assessment of existing infrastructure/security measures with respect to RBI Guidelines vide its Circular dated 02-Jun-2016.

a) Understand the present infrastructure, architecture, Security Policies, security measures etc. in consultation with concerned teams/officials and also with top management of the Bank.

b) Review the existing Processes, Procedures and systems for their sufficiency of controls.

c) Review the existing SOC Operations

d) Identify gaps in Bank's Cyber threat detection mechanisms

e) Suggest controls under Administrative, Technical and Physical categories to mitigate the gaps.

2. Drafting Cyber Security Policy for the Bank

a) Reviewing existing Information Security Management System (ISMS) policy framework of the Bank

b) Drafting separate Cyber security policy and Cyber Crisis management plan in line with Reserve Bank of India guidelines and other industry best practices.

c) Suggest Cyber crisis Management team structure

d) Providing Measurement matrix template to evaluate effectiveness of the Cyber Crisis Management Plan

e) Creating Cyber incident scenarios and Conducting two Mock drills.

f) Review the mock drills results and suggest improvements

g) Revise Cyber Crisis Management plans.

3. Formulating Digital Evidence Policy

Digital evidence is similar to any other form of legal proof with the following requirements/features :

a) it needs to withstand challenges to its integrity

b) its handling must be carefully tracked and documented

c) it must be suitably authenticated by concerned personnel as per legal requirements

A suitable Digital Evidence policy, specially focusing on preservation of digital evidence, needs to be formulated keeping in view the banking scenario and to comply with RBI guidelines (Sir G G Committee recommendation and recent circular dated 02-Jun-2016).

4. Assisting in implementing Cyber-Security Operation Centre (C-SOC) through formal tender process

Understanding of existing SOC in operation in the bank and implementation of C-SOC through formal tender process, covering the following major expectations :

a) Ability to Protect critical business and customer data/information, demonstrate compliance with internal guidelines, country regulations and laws

b) Ability to Provide real-time/near-real time information on and insight into the security posture of the bank

c) Ability to Effectively and Efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery

d) Ability to assess threat intelligence and the proactively identify/visualize impact of threats on the bank

e) Ability to know who did what, when , how and preservation of evidence

f) Integration of various log types and logging options into SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.

5. Implementation of effective Incident Management Response Structure and Process

Understanding of existing Incident Management Response structure presently in practice in the Bank and providing suggestion in order to comply with the RBI guidelines dated 02-Jun-2016.

6. Review and updation of existing Minimum Baseline Security Documents to include cyber security aspects.

Review of existing Minimum Baseline Security Document and updation to cover a list of requirements to be put in place to achieve baseline cyber-security/resilience.

18. Bidder Eligibility Criteria.

a) The bidder should be either a Government Organization/PSU/PSE/ partnership firm or a limited Company under Indian Laws or /and an autonomous Institution approved by GOI/RBI promoted

b) The bidder should have been in existence in India for minimum three years as on 30-06-2016.

c) The bidder should have a minimum average annual turnover of Rs. 10.00 crores (Rupees Ten Crores) during last three financial years 2013-14, 2014-15 and 2015-16.

d) The bidder should have made net profits for the last 3 financial years viz. 2013-14, 2014-15 and 2015-16.

e) The bidder should have at least three (3) years experience in offering Information Security Services such as Security assessment, defining security policies procedures & baselines, Gap assessment as per international standards, Risk Assessment, security consulting assignments etc. to public sector Banks in India.

f) The Bidder must have experience of conducting Data Centre Security Assessment to at least -2 BFSI institutions in India out of which at least -1- should be a Bank in India with minimum 500 branches during past 3 years.

g) The Bidder must have at least Two (2) Security Consultants with qualifications such as ISO 27001/ISO 22301 Lead Auditors as employees.

h) The Bidder must have at least Three (3) CISA/CISSP/CEH Certified professionals as employees.

i) The Bidder must have at least 5 CCNA/CCNA Security/CCNP/CCSP/CCIE certified engineers

j) The firm should not be blacklisted / barred by Government of India or any regulatory body in India.

k) The Bidder or its parent company or its subsidiary should not be existing System integrator maintaining IT infrastructure at Data Centre and Disaster Recovery site of the Bank.

l) Vendor must not be a NPA holder in any Bank/Financial Institution.

19. Earnest Money Deposit.

Subject to compliance of Response Submission Process as elucidated in the RFP, the intending bidders should pay along with bids an Earnest Money Deposit of Rs.50,000/- (Rupees Fifty thousand only). The EMD shall be paid by Demand Draft / Banker's Cheque / Pay Order drawn in favor of '**Central Bank of India"** payable at Mumbai. The EMD will not carry any interest.

The EMD made by the bidder will be forfeited if:

a. The bidder withdraws his tender before processing of the same.
b. The bidder withdraws his tender after processing but before acceptance of "Letter of appointment" issued by Bank.
c. The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.
d. The bidder violates any of the provisions of the terms and conditions of this tender specification.
e. The EMD will be refunded to
   - The successful bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee in the Bank format for 10% of the contract value (valid till the end of assignment period) with 3 (three) months claim period.
   - The unsuccessful bidders, only after acceptance of the "Letter of Appointment" by the selected bidder.

20. Application Money.

The intending bidders should pay an Application Money of Rs.5,000/- (Rupees Five thousand only) on or before the prebid meeting. The application money shall be paid by Demand Draft / Banker's Cheque / Pay Order drawn in favor of '**Central Bank Of India"** payable at Mumbai. The application money is non-refundable.

21. Submission of Bids

The bids shall be in two parts viz. Technical Proposal and Commercial Proposal. Both Technical and Commercial Proposals shall be submitted in separate sealed envelopes super-scribing

"TECHNICAL PROPOSAL FOR Appointment of Security Consultant: TENDER REFERENCE NO. 226"on top of the envelope containing the technical bid and **"COMMERCIAL PROPOSAL FOR Security Consultant: TENDER REFERENCE NO.226"** on top of the envelope containing commercial bid.

These two separate sealed envelopes should be put together in the sealed master envelope superscribing **"PROPOSAL for Appointment of Security Consultant for implementing Cyber Security Framework: TENDER REFERENCE NO. 226"**

The Technical Proposal will be evaluated for technical suitability. Commercial Proposal shall be opened only for the short-listed bidders who have qualified in the Technical Proposal evaluation.

The Technical Proposal shall contain the requirement of the Bank as along with Annexure–A, C, D and E. A copy of the Commercial Proposal masking the prices is to be submitted along with the Technical Proposal.

The EMD is to be submitted along with the Technical Proposal.

Application money of Rs.5000/- (Rupees Five thousand only) is to be submitted on or before the pre-bid meeting.

The Technical Proposal shall be organized and submitted as per the following sequence:

- Table of Contents (list of documents enclosed).
- EMD (Earnest Money Deposit).
- Application money (if not submitted earlier).
- Technical proposal detailing the scope, approach and deliverables for the scope of work specified in the document and manpower estimated to be deployed along with Annexure D.
- Compliance certificate for all the terms and conditions as per Annexure-C.
- All copies of certificates, documentary proofs etc.
- A CD containing soft copy of the technical proposal.
- Annexure A.
- Masked Annexure B.

The Commercial Proposal shall be submitted as per Annexure B. The bidder shall submit the Proposals properly filed so that the papers are not loose. The Bidder shall submit the proposal in suitable capacity of the file such that the papers do not bulge out and tear during scrutiny.

All the relevant pages of the proposals (except literatures, datasheets and brochures) are to be numbered and be signed by authorized signatory on behalf of the Bidder. The number should be a unique running serial no. across the entire document.

The bidder has to submit a soft copy of the technical proposal in a CD. It should be noted that in case of any discrepancy in information submitted by the bidder in hard-copy and soft-copy, the hard-copy will be given precedence. However, in case of non-submission of any hard copy document, if the same is found submitted in the soft-copy, Bank reserves right to accept the same at its discretion.

The Bids shall be addressed and submitted to:

Asst. General Manager-IT
Central Bank Of India
Central Bank Building
1st floor, DIT, Sector-11
CBD Belapur, Navi Mumbai-400614

The bids (arranged as mentioned above) are to be submitted at the above address, marked with the tender number before the due date & time as specified. The bid submitted anywhere else is liable to be rejected.

It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing/email only and should be to the nominated point of contact.

Bidders should provide their E-mail address in their queries without fail. The bidder will submit an undertaking specifying that the bidder has obtained all necessary statutory and obligatory permission to carry out project works, if any.

The proposal should be prepared in English. The e-mail address and phone/fax numbers of the bidder should also be indicated on the sealed cover.

Formats of Bids- The bidders should use the formats prescribed by the Bank in the RFP for submitting both technical and commercial bids.

22. General Terms and Conditions

Adherence to Terms and Conditions: The bidders who wish to submit responses to this RFP should note that they should abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the respondents, such responses may be disqualified and may not be considered for the selection process.

Execution of SLA/NDA & Confidentiality agreement

The Security consultant and Bank should execute

a. **Service Level Agreement**. This would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and;
b. **Non-disclosure Agreement**. The Security Consultant should execute the SLA and NDA as attached herewith within one month from the date of acceptance of Letter of Appointment.
c. **Confidentiality agreement by the individual representatives involved in the on-site assignment at Bank's premises.**

Compliance to Information Security

a. The Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, storage tapes or any other media out of Bank's premise without written permission from Bank.

b. The Bidder personnel shall follow Bank's Information Security Management System policy and instructions in this behalf.

c. Bidder acknowledges that Bank's business data and other Bank proprietary information or materials, whether developed by Bank or being used by Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to Bank; and Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Bidder to protect its own proprietary information. Bidder recognizes that the goodwill of Bank depends, among other things, upon Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder could damage Bank. By reason of Bidder's duties and obligations hereunder, Bidder may come into possession of such proprietary information, even though Bidder does not take any direct part in or furnish the Services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by this Contract. Bidder shall use such information only for the purpose of performing the Services.

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

Project Timelines

The entire activities which are under the scope of this RFP should be completed within a maximum period of six (6) months from the date of the PO issued to the selected bidder.

The selected Bidder shall furnish a schedule of assessment encompassing its entire scope, discuss the same with the Bank officials and arrive finally at a mutually agreed assessment/implementation schedule within the overall ambit of six months time.

For Gap remediation, Consultant should provide necessary support and hand-holding assistance including consultancy services as defined in the scope till the gaps are rectified.

The above timelines are tentative and may be extended at the discretion of the Bank at no extra cost to the Bank.

Extension of the Contract

1. The term of this Contract shall be initially for a period of **six months from the date of signing of agreement.**

2. Bank shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Bidder, at least One week before the expiration of the term hereof

whether it will grant the Bidder an extension of the term. The decision to grant or refuse the extension shall be at the sole discretion of Bank.

Other Terms and Conditions

a. **Bank reserves the right to:**
- Reject any and all responses received in response to the RFP.
- Waive or Change any formalities, irregularities, or inconsistencies in proposal format delivery.
- To negotiate any aspect of proposal with any bidder and negotiate with more than one bidder at a time.
- Extend the time for submission of all proposals.
- Select the most responsive bidder (in case no bidder satisfies the eligibility criteria in totality).
- Select the next most responsive bidder if negotiations with the bidder of choice fail to result in an agreement within a specified time frame.
- Share the information/ clarifications provided in response to RFP by any bidder, with any other bidder(s) /others, in any form.
- Cancel the RFP/Tender at any stage, without assigning any reason whatsoever.
- Interview the personnel being deployed on the project.

b. **Substitution of Project Team Members-** During the assignment, the substitution of key staff identified for the assignment will not be allowed unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the vendor can do so only with the concurrence of the Bank by providing other staff of same level of qualifications and expertise.

c. **Professionalism and Conflict of interest-** The Security Consultant should provide professional, objective and impartial advice at all times and hold the Bank's interests paramount and should observe the highest standard of ethics while executing the assignment.

The Bank further requires that Bidder/Security Consultants provide professional, objective and impartial advice and at all times hold the Bank's interests paramount, strictly avoid conflicts with other assignment/jobs or their own corporate interest and act without any consideration for future work.

A Security Consultant that has a business or family relationship with a member of the Bank's staff who is directly or indirectly involved in any part of the project shall not be awarded the Contract, unless the conflict stemming from this relationship has been resolved in a manner acceptable to the Bank throughout the selection process and the execution of the Contract. Bidder/Security Consultants have an obligation to disclose any situation of actual or potential conflict that impacts their capacity to serve the best interest of their Bank, or that may reasonably be perceived as having this effect. Any such disclosure shall be made as per the forms of technical proposal provided herewith. If the Security Consultant fails to disclose said situations and if the Bank comes to know about any such situation at any time, it may lead to the disqualification of the Security Consultant during bidding process or the termination of its contract during execution of the assignment.

d. **Adherence to Standards**: The Security Consultant should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities.

e. The Bank reserves the right to conduct an audit/on-going audit of the consulting services provided by the Security Consultant.

f. The Bank reserves the right to ascertain information from the banks and other institutions to which the bidders have rendered their services for execution of similar projects.

g. **EXPENSES**- It may be noted that Bank will not pay any amount/expenses / charges / fees / travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses other than the "Agreed Professional Fee".

h. The bidder cannot change the people assigned to a particular piece of work till such work is complete unless consented in written by the Bank.

i. The bid should contain the resource planning proposed to be deployed for the project which includes, inter-alia, the number of personnel, skill profile of each personnel, duration etc.

j. The bidder is expected to quote for the prices of the services with the applicable taxes (except service tax) as on the date of bid submission. Any upward / downward revision in the tax rates from the date of the bid submission will be to the account of the Bank.

k. **Terms of Payment**- The security consultant is expected to quote for a fixed price for the project based on the scope of work defined by the Bank. The full payment will be made by the bank post submission of all deliverables and acceptance of reports.

l. **Performance Bank Guarantee** : The successful bidder will have to give Performance Bank Guarantee for 10% of the total project cost, while submitting the acceptance of order. The

validity of the Performance Bank Guarantee should be for 12 months with a claim period of additional three months. If required, it should be renewed till completion of the assignment without any additional cost to the Bank.

n. Penalty: If the selected bidder fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the final contract, the Bank reserves the right to recover penalty/liquidated damages of 1% of the contract value per week or part thereof, subject to a maximum of 10% of contract value as Liquidated Damages for non-performance/delayed performance. The bank also reserves the right to impose / waive any such penalty.

o. Authorized Signatory- The selected bidder shall indicate the authorized signatories who can discuss and correspond with the bank, with regard to the obligations under the contract.

The selected bidder shall submit at the time of signing the contract, a certified copy of the extract of the resolution of their Board, authenticated by Bank Secretary, authorizing an official or officials of the Bank or a Power of Attorney copy to discuss, sign agreements/contracts with the Bank. The bidder shall furnish proof of signature identification for above purposes as required by the Bank.

p. Applicable Law and Jurisdiction of court- The Contract with the selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Mumbai (with the exclusion of all other Courts).

q. Arbitration: In case of any dispute, Bank may appoint an arbitrator, which would be accepted by the Bidder. The decision of the arbitrator would be final and binding on both the parties. The jurisdiction of the court would be Mumbai.

r. Cancellation of Contract and Compensation- The Bank reserves the right to cancel the contract of the selected bidder and recover expenditure incurred by the Bank on the following circumstances:

- The selected bidder commits a breach of any of the terms and conditions of the bid/ contract.
- The bidder goes into liquidation voluntarily or otherwise.
- An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
- The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
- If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out bidding process for the execution of the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order.

u. Subcontracting- The Security Consultant shall not subcontract or permit anyone other than its personnel or related firms / entities to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.

v. Limitation of Liability- The aggregate liability of the Security Consultant in connection with this Agreement, the consultancy services provided by the Security Consultant for the specific scope of work document, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise) and including any and all liability shall be the actual limited to the extent of the value paid to the Security Consultant in the contract for the specific scope of work document.

w. INDEMNITY- Bidder shall indemnify and hold harmless the Bank and its personnel from and against any loss, dues, fine, penalty, compensation, cost, damage, liability and expenses (including but not limited to attorney's fees) incurred relating to any claims arising out of or in any way relating to the Services or this Agreement.

x. FORCE MAJEURE -For the purpose of this contract, "Force Majeure" means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable and not brought about by or at the instance of the Party claiming to be affected by such events and which has caused the non-performance or delay in performance, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other extreme adverse weather conditions, strikes, lockouts or other industrial action(except where such strikes, lockouts or other industrial action are within the power of the party invoking Force majeure to prevent), confiscation or any other action by Government agencies.

i. Force Majeure shall not include (a) any event which is caused by the negligence or intentional action of a Party or by or of such Party's sub-consultants or agents or employees, nor (b) any event which is a diligent party could reasonably have been expected both to take into account at the time of the conclusion of this contract, an avoid or overcome in the carrying out of its obligations hereunder.

ii. Force Majeure shall not include insufficiency of funds or inability to make any payment required hereunder.

iii. A party affected by an event of force majeure shall continue to perform its obligations under the contract as far as is reasonably practical, and shall take all reasonable measures to minimize the consequences of any event of force majeure.

iv. A party affected by an event of force majeure shall notify the other party of such event as soon as possible, and in any case not later than 14 days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of restoration of normal conditions as soon as possible.

This provision shall survive the termination of this Agreement for any reason.

23. Bid Evaluation Criteria

Evaluation of Technical Bid

First, Technical bid documents will be evaluated for fulfillment of eligibility criteria. Technical bids of only those Bidders who fulfill the eligibility criteria fully as per Annexure-A will be taken up for further evaluation/selection process. A maximum of 100 marks will be allocated for the technical bid. The evaluation of functional and technical capabilities of the Bidders of this RFP will be completed first as per the following guidelines. The technical proposals only will be subjected for evaluation at this stage. The Bidders scoring less than 70 marks (cut-off score) out of 100 marks in the technical evaluation shall not be considered for further selection process. Once the evaluation of technical proposals is completed, the Bidders who score equal to, or more than the prescribed cut-off score of 70 will only be short listed. The evaluation of technical proposals, among other things, will be based on the following:

 Prior experience of the Bidder in undertaking projects of similar nature.

 Professional qualifications and experience of the key staff proposed/ identified for this assignment.

 Methodology/Approach proposed for accomplishing the proposed project, Activities / tasks, project planning, resource planning, effort estimate etc.

Various stages of technical evaluation are presented below:

1. Eligibility evaluation as per the criteria mentioned in Clause 19 above.

2. Evaluation of technical proposals of Bidders qualified in eligibility evaluation, based on response and presentation

3. Arriving at the final score on technical proposal.

Presentation-cum-Interview

The Bidders who are qualified in eligibility evaluation, have to give presentation/interactions before panel of representatives of Bank on the methodology/ approach, time frame for various activities, strengths of the Bidders in carrying out the tasks as per the scope of the RFP. The technical competence and capability of the Bidder should be clearly reflected in the presentation. If any short listed Bidder fails to make such presentation, he will be eliminated from the evaluation process. At the sole discretion and determination of the Bank, the Bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.

Technical Bid Evaluation Criteria

The criteria for evaluation of technical bids is as under.

Criteria	Evaluation Parameters	Max Marks	Documents to be submitted	Min. Marks required
Credentials				
The number of years of experience of conducting Data Centre Infrastructure Audit /security review in last 5 years in Banks.	For each year of experience	2	Copies of Work order and/or Client letter.	
	Maximum marks	10		6
The number of Information / Cyber / IT Security Policy reviews assignments carried out.	For each assignment	3	Copies of Work order and/or Client letter.	
	Maximum marks	9		3
The number of VAPT of internet facing infrastructure carried out in BFSI.	For each assignment to BFSI Institution	3	Copies of Work order and/or Client letter.	
	Additional marks for a Bank in India	3		
	Maximum marks	12		6
The number of Data Centre Infrastructure Audits of BFSI/Banks carried out in India	For each assignment	3	Copies of Work order and/or Client letter.	
	Maximum marks	9		6
The number of Security Operations Centre Reviews	For each consultancy to BFSI Institution	3	Copies of Work order and/or Client letter.	
	Additional marks for a Bank in India	3		
	Maximum marks	15		6
Sub-total (Credentials		55		
Manpower				
The number of ISO22301/ ISO 27001 Lead Auditors employed by the Bidder	For each certified employees	2	1. Copy of relevant Certificate; 2. Proof of employment with the Bidder.	
	Maximum marks	10		4
The number of CISA/CISSP/CEH Certified personnel employed by the Bidder	For each certified employee	1		
	Maximum marks	5		3
The number of CCNA/CCNA Security/CCNP/CCSP/CCIE, CCIE Security certified engineers employed by the Bidder	For each CCNA, CCNA-Security certified employee	1		
	For CCNP/CCSP	2		
	For CCIE / CCIE-Security	5		
	Maximum marks	10		5
Sub total (Manpower)		25		
Methodology & Approach	Demonstration of in-depth understanding of the Bank's project requirements through the technical proposal	20	Subjective evaluation based on technical proposal and	15

	and presentation, with detailed broken-down activities to be performed, effort estimation, manpower to be deployed.		presentation	
TOTAL MARKS		100		

NOTE

1: Experience of last -5- years only will be counted in the Technical Evaluation of the Bids.

2: For manpower consideration, the Employee should be on the payroll of the Bidding company. For this proof in the form of employment letter duly accepted by the employee or suitable declaration jointly signed by the Employer and Employee stating date of joining on the Bidding company's letterhead should be submitted.

Bank may, at its sole discretion, decide to seek more information from the Respondents in order to normalize the bids. However, Respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.

Cut - Off score for technical bid will be 70 marks.

In case there is only one bidder having technical score of 70 or more, Bank may, at its discretion, also consider the next highest technical scorer with minimum score of 60. In case, no Bidder is having technical score of 70 or more, Bank may, at its discretion, qualify 2 top scoring Bidders with minimum score of 60 in technical evaluation and compute the "Score" as per the evaluation criteria.

Annexure-A (Technical Bid format) to be submitted by Bidders should contain detailed responses to each of the above evaluation criteria along with documentary proofs as specified there against.

Commercial Bid Evaluation Criteria

Only those Bidders qualified in technical evaluation as mentioned above will be short-listed for commercial evaluation.

If necessary, Bank reserves the right to form an appropriate negotiation committee to have negotiation with the L1 vendor. Bank will award the contract to the successful Vendor whose bid has been determined as the Lowest Commercial bid (L1) through the process of this commercial evaluation.

Bank reserves the right to modify / amend the evaluation process at any time during the bid process, without assigning any reason, whatsoever and without any requirement of intimating the bidders of any such change.

24. Annexures

24.1. Annexure A- Technical Proposal Format

Particulars to be provided by the bidder in the technical proposal. Tender Ref. No. CO:DIT:PUR:2016-17:226

Sr. No	Particulars	Details to be furnished by the bidder
1	Name of the bidder	
2	Date of establishment and constitution. Certified copy of "Partnership Deed" or "Certificate of Incorporation/commencement of business" should be submitted. For entities other than partnership firm and limited company, other relevant documents to be submitted.	
3	Location of Registered Office /Corporate Office/ Mumbai office with addresses.	
4	Mailing address of the bidder	
5	Names and designations of the persons authorized to make commitments to the Bank	
6	Telephone and fax numbers of contact persons	
7	E-mail addresses of contact persons	
8	Details of : Description of business and business background Service Profile & client profile Domestic & International presence Alliance and joint ventures	
9	Gross annual turnover of the Bidder (not of the group) Year 2013-14 Audited Year 2014-15 Audited Year 2015-16 Audited (Copy of audited financial statements for above years to be submitted)	

Sr. No	Particulars	Details to be furnished by the bidder
10	Net Profit of the bidder (not of the group) Year 2013 - 14 Year 2014 – 15 Year 2015 – 16 (Copy of audited financial statements for above years to be submitted)	
11	Experience Details of last -5- years (For item nos. 11 a to 11 d, Name of the organization, time taken for execution of the assignment and documentary proofs in the form of copy of work order and Copy of certification are to be furnished)	
11 a	Experience of conducting Data Centre Infrastructure Audit /security review in last 5 years in Banks	
11 b	Experience of Information/Cyber/IT Security Policy reviews assignments carried out.	
11 c	Experience of VAPT of internet facing infrastructure carried out in BFSI.	
11 d	Experience of conducting Security Operations Centre Reviews	
12	Details of the similar assignments on hand as on date (Name of the Bank, time projected for execution of the assignment and documentary proofs such as work order are to be furnished)	
13	Name of the Engagement Manager & Overall person responsible (team leader) identified for this assignment and his professional qualifications and experience/expertise Details of similar assignments handled by the said team leader. Documentary proofs for all the assertions are to be enclosed.	
14	Names of the other team members identified for this assignment and their professional qualifications and experience/expertise. (Should possess qualifications as mentioned in the RFP) Documentary proofs for all the assertions in the form of Certificates, CVs, employment letter to be enclosed.	

Sr. No	Particulars	Details to be furnished by the bidder
15	Names of the staff members and their certifications as per the following: (Copy of relevant certification and proof of employment should be enclosed)	
A	ISO22301/ISO 27001 certified Lead Auditors	
B	CISA/CISSP/CEH certified employees	
C	CCNA/CCNA Security/CCNP/CCSP/CCIE, CCIE Security certified engineers	
16	Estimated work plan and time schedules for providing services for this assignment.	
17	Effort estimate and elapsed time are to be furnished.	
18	Details of inputs, infrastructure requirements required by the Bidder to execute this assignment.	
19	Details of the Bidder's proposed methodology/approach with reference to the scope of work.	
20	Details of deliverables, other than the deliverables with reference to the scope of work.	

Declaration:

a. We confirm that we will abide by all the terms and conditions contained in the RFP.
b. We hereby unconditionally accept that Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in short listing of bidders.
c. All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process.
d. We confirm that this response, for the purpose of short-listing, is valid for a period of six months, from the date of expiry of the last date for submission of response to RFP.
e. We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Place :

Date :

Seal & Signature of the bidder:

24.2. Annexure B- Commercial Bid Format

The Security Consultant has to quote for the fees based on the scope of work. Prices below are to be quoted exclusive of applicable taxes.

S. No.	Major Activities	Quantity	Unit Cost	Total Cost of Assignment
1	Performing Gap Assessment of Bank's existing infrastructure and assisting in remedial measures to comply with respect to RBI Guidelines dated 02-Jun-2016.	1		
2	Drafting Cyber Security Policy as per international best practices.	1		
3	Formulating Cyber Crisis Management Plan.	1		
4	Formulating Digital Evidence Policy	1		
5	Assisting in implementing Cyber-Security Operation Centre (C-SOC) through formal tender process – Drafting of RFP	1		
6	Implementation of effective Incident Management Response Structure and Process	1		
7	Review and updation of existing Minimum Baseline Security Documents to include cyber security aspects.	1		
8	Others (if any). Pl. specify	1		

Amount in Words : _____.

Note:

- The price quoted for the project should be inclusive of taxes and charges except service tax. Service tax will be payable actual.
- The cost should be all inclusive including usage of tools etc.
- Figures from Grand Total would be considered for evaluation of the bid as per Evaluation criteria.
- The base location for the project execution would be Mumbai.
- The Security Consultant will have to work as per the timing of the Bank
- All prices to be valid for a period of 1 year from the date of contract execution / signing.

Place:

Date : Seal & Signature of the Bidder

24.3. Annexure C- Compliance Certificate

Compliance Certificate

To, Date :

Asst. General Manager
Central Bank Of India
DIT, Central Office,
CBD Belapur

Dear Sir,

Ref: -

1. Having examined the Tender Documents including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide consultancy in conformity with the said Tender Documents and in accordance with our proposal and the schedule of Prices indicated in the Price Bid and made part of this Tender.

2. We confirm that this offer is valid for six months from the last date for submission of Tender Documents to the Bank.

3. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

4. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

5. We agree that the Bank is not bound to accept the lowest or any Bid that the Bank may receive.

6. We have never been barred/black-listed by any regulatory / statutory authority in India.

Signed Dated

Seal & Signature of the bidder

Phone No.: Fax: E-mail:

24.4. Annexure D- Proposed Team Profile

Sl No	Name of Proposed Engagement Manager /Proposed Team Member	Professional Qualifications	Certifications / Accreditations	Experience in a. Information /Cyber Security Policy review b. Performing gap assessment as per international standards c. Formulating Cyber Crisis Management Plan d. Security Operations Centre Review e. Conducting Mock Cyber Security Drills	IT Security Expertise In terms of years and areas of expertise	Experience in other Information Security areas such as Application audits, VAPT etc
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

24.5. Annexure E- List of Certified Employees

Sl No	Name of Employee	Date of Joining	Date of Certifications / Accreditions		
			ISO22301 / ISO 27001 LA	CISA/ CISSP / CEH	CCNA/ CCNA Security/ CCNP/ CCSP/ CCIE, CCIE Security
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

24.6. Annexure F – Experience Details

DETAILS OF WORK EXPERIENCE AS PER ELIGIBILITY AND TECHNICAL EVALUATION CRITERIA

Sl. No.	Name of the Client	Client segment Bank or BFSI or Others	Date of PO	Date of completion of assignment	Date of Certification (if applicable)	Name of Lead consultant	Contact person details of the client	Page Ref.

24.7. Annexure G – Estimated Efforts and Time Proposed

S. No.	Activities as per Scope of Work	Time Proposed	Effort in Man days	Number of team members to be deployed	Remarks
1	Performing Gap Assessment of Bank's existing infrastructure and assisting in remedial measures to comply with respect to RBI Guidelines dated 02-Jun-2016.				
2	Drafting Cyber Security Policy as per international best practices.				
3	Formulating Cyber Crisis Management Plan.				
4	Formulating Digital Evidence Policy				
5	Assisting in implementing Cyber-Security Operation Centre (C-SOC) through formal tender process – Drafting of RFP				
6	Implementation of effective Incident Management Response Structure and Process				
7	Review and updation of existing Minimum Baseline Security Documents to include cyber security aspects.				
8	Other activities (if any). Pl. specify				

24.8. Annexure I - Confidentiality Agreement

Document ID: CBI ISMS-L3-7- Confidentiality Agreement

Confidentiality Agreement

This agreement is entered into as of this_____ day of _____2016, by and between the bank and _____.

Where, the undersigned is desirous of accessing restricted / confidential / internal information / data of the bank; and therefore, the undersigned agree to the following:

1. We will not disclose or make available to any third party of the bank, any confidential, internal or proprietary contents of the knowledge or information of the bank or information about its clients maintained on the knowledge or information bases of the bank, nor will I grant direct access to such information or information sharing processes unless :
   - ► The concerned information owner in the bank gives them expressed, advanced and written permission as to each and every third party;
   - ► Each and every employee of the third party enters into a written agreement in the form of this Agreement.
2. Such confidentiality will be maintained by us during the period of our employment / contract with the bank as well as after the termination of such employment / contract.
3. We have read and understood the Bank's IS Security Policies and Procedures and agree to abide by it.
4. We will protect confidential / internal information of the bank from loss and unauthorized use and manipulation.

Signature ( )

_____

Name ( )

24.9. ANNEXURE J - NON-DISCLOSURE AGREEMENT

NON-DISCLOSURE AGREEMENT

This Agreement made at _____, on this _____ day of _____ 2016.

BETWEEN

_____ a company incorporated under the Companies Act, 1956 having its registered office at _____ (hereinafter referred to as "-----" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the **ONE PART**;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office, Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as "**CBI**" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the **OTHER PART**

and **CBI** are hereinafter individually referred to as party and collectively referred to as "the Parties". Either of the parties which discloses or receives the confidential information is respectively referred to herein as Disclosing Party and Receiving Party.

WHEREAS:

The Parties intend to engage in discussions and negotiations concerning the establishment of a business relationship between them. In the course of such discussions and negotiations, it is anticipated that both the parties may disclose or deliver to either of the Parties certain or some of its trade secrets or confidential or proprietary information, for the purpose of enabling the other party to evaluate the feasibility of such business relationship (hereinafter referred to as "**the Purpose**").

NOW, THEREFORE, THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. **Confidential Information:** "Confidential Information" means all information disclosed/ furnished by either of the parties to another Party in connection with the business transacted/to be transacted between the Parties and/or in the course of discussions and negotiations between them in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof.

   Either of the Parties may use the Confidential Information solely for and in connection with the Purpose.

Notwithstanding the foregoing, "Confidential Information" shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving it

from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, or (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

2. **Non-disclosure:** The Receiving Party shall not commercially use or disclose any Confidential Information or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to Security Consultants only if the Security Consultant has executed a Non-disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or Security Consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefore.

Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

3. **Publications:** Neither Party shall make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the other Party.

4. **Term:** This Agreement shall be effective from the date hereof and shall continue till establishment of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease any and all disclosures or uses of Confidential Information; and at the request of the Disclosing Party, the Receiving Party shall promptly return or

destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

Notwithstanding anything to the contrary contained herein the confidential information shall continue to remain confidential until it reaches the public domain in the normal course.

5. **Title and Proprietary Rights:** Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

6. **Return of Confidential Information:** Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.

7. **Remedies:** The Receiving Party acknowledges that if the Receiving Party fails to comply with any of its obligations hereunder, the Disclosing Party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The Receiving Party agrees that, in addition to all other remedies provided at law or in equity, the Disclosing Party shall be entitled to injunctive relief hereunder.

8. **Entire Agreement, Amendment, Assignment:** This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

9. **Governing Law and Jurisdiction:** The provisions of this Agreement shall be governed by the laws of India. The disputes, if any, arising out of this Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

10. **General:** The Receiving Party shall not reverse-engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder. All Confidential Information is provided "as is". In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by the parties constitutes any representation, warranty, assurance, guarantee or inducement by either party to the other with respect to the fitness of such Confidential Information for any particular purpose or infringement of trademarks, patents, copyrights or any right of third persons.

11. **Indemnity:** The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party etc., officers, employees, agents or consultants.

IN WITNESS WHEREOF, the Parties hereto have executed these presents the day, month and year first hereinabove written.

For and on behalf of

_____

Name of Authorized signatory:

Designation:

For and on behalf of

CENTRAL BANK OF INDIA

_____

Name of Authorized signatory:

Designation:

End of Document