RFP FOR ENGAGEMENT OF CYBER SECURITY CONSULTANT

September 23, 2019

RFP REFERENCE NO. : NHB(ND)/AAD/A10563/2019

All Audits Department
Head Office, National Housing Bank
Core 5-A, 3rd Floor, India Habitat Centre, Lodhi Road,
New Delhi – 110 003
Phone: 011-2464 9031-35
E-Mail: amit.sinha@nhb.org.in ; prabhat.ranjan@nhb.org.in

GLOSSARY

Abbreviation	Description
NHB	National Housing Bank
HO	Head Office, Delhi
RRO	Regional Representative Office
PSU	Public Sector Unit
SBI	State Bank of India and its associates (before merger)
PSB	Public Sector Bank /Nationalized Bank (total 20)
EMD	Earnest Money Deposit
RFP	Request For Proposal
PBG	Performance Bank Guarantee
AMC	Annual Maintenance Cost

Interpretation: *the terms RFP, Tender, Bid have been used interchangeably and it shall be treated as one and the same for the purpose of this RFP document. All clarifications, amendments, modifications, supplemental RFP that may be issued in relation to this RFP shall be treated as part and parcel of the RFP and shall together constitute the RFP document.*

Table of Contents

1. IMPORTANT BID DETAILS

1.	Date of commencement of sale of Bidding/Tender/RFP Documents	23.09.2019
2.	Pre-Bid meeting with Bidders (Date and Time)	1100 Hrs 03.10.2019
3.	Last date and time for sale of Bidding Documents	1800 Hrs 21.10.2019
4.	Last date and time for receipt of Bidding Documents	1800 Hrs 21.10.2019
5.	Date and Time of Technical Bid Opening	1500 Hrs 22.10.2019
6.	Cost of RFP(Non-refundable)	10,000/-
7.	Earnest Money Deposit Amount	1,00,000/-
8.	Place of opening of Bids	National Housing Bank, All Audits Department Head Office Core 5-A, 3rd Floor, India Habitat Centre, Lodhi Road, New Delhi – 110003

Note: -

- **Technical Bids will be opened in the presence of Bidders who choose to attend as above. The above schedule is subject to change. Notice of any changes will be provided through e-mail from designated contact personnel only or publishing on NHB's website. Further, please note that Commercial Bid opening Date, Time & Venue will be intimated to the technically qualified Bidders at a later date.**
- **All data/information, submitted vide documentary proofs/company records along with this RFP, must be reported & will be treated as on date of publication of this RFP.**

2. National Housing Bank

National Housing Bank (NHB), a statutory body under Govt. of India, established under an Act of the Parliament.

a. NHB has been established to achieve, inter alia, the following objectives –
   - To promote a sound, healthy, viable and cost effective housing finance system to cater to all segments of the population and to integrate the housing finance system with the overall financial system.
   - To promote a network of dedicated housing finance institutions to adequately serve various regions and different income groups.
   - To augment resources for the sector and channelize them for housing.
   - To make housing credit more affordable.
   - To supervise the activities of housing finance companies based on regulatory and supervisory authority derived under the Act.
   - To encourage augmentation of supply of buildable land and also building materials for housing and to upgrade the housing stock in the country.
   - To encourage public agencies to emerge as facilitators and suppliers of serviced land, for housing.

b. The head office of NHB is located in New Delhi and a regional office located at Mumbai. It has representative offices located at Hyderabad, Bengaluru, Kolkata and Ahmedabad.

3. Purpose:

- National Housing Bank (NHB) (hereinafter referred to as the Bank) proposes to invite Request for Proposal (RFP) tenders from the eligible vendors to provide following services:

  a) To review preparedness of the Bank with respect to RBI Circulars / advisories on Cyber Security Framework (issued from 2016 to 2019) and to vet self-assessment of gaps vis-à-vis baseline security & resilience requirement;

  b) To design and develop Cyber Security Policy (CSP) & Procedures along with Cyber Crisis Management Plan (CCMP) and

  c) To prepare the requirement for setting up of Cyber Security Operation Centre (C-SOC) as per RBI guidelines as also to facilitate the process for selection of a suitable vendor for setting up CSOC (viz. preparation of terms of proposal/RFP, eligibility criteria, scope of work and finalization etc.)

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

  Subject to any law to the contrary, and to the maximum extent permitted by law, NHB 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 NHB or any of its officers, employees, contractors, agents, or advisers.

4. Objective:

The objective of this assignment is to comply to the circulars and advisories issued by CSITE, RBI and to create a robust Information Security System (Cyber Security Framework, Cyber Security Operation Centre, Incident Reporting Mechanism etc.) in the Bank to fight against Cyber Security Threats.

5. Scope of Work:

Scope of Work	**Deliverables**	**Delivery Timelines**
1. Review of Information Security/Cyber Security vis-à-vis RBI Circular on Cyber Security Framework 1.1. Review of preparedness of the Bank vis-à-vis RBI Circular on Cyber Security Framework in Banks. 1.2. Vetting of Self-assessment of gaps vis-à-vis Baseline Security & Resilience Requirements.	Gap Assessment Report as envisaged in the RBI Circular with recommended action plan and proposed timelines.	**4 Weeks from the Date of Purchase Order**

2. Preparation of Cyber Security Policy 2.1. Preparation of Cyber Security Policy& Procedures, Cyber Crisis Management Plan as part of above policy.	Cyber Security Policy and Procedures Cyber Crisis Management Plan Changes to Existing Policies, Procedures	
3. Review of IT infrastructure from the point of view of Information/Cyber Security. 3.1. Review / update Information Security Policies, Procedures and Guidelines. 3.2. Review of the Current Security Architecture and Security Technology of the organization. 3.3. Review the process for Vulnerability Assessment [VA] and Penetration Testing [PT] for Servers and Network/Security devices, Application Security Testing [Web and Mobile Appsec] being done for the bank. 3.4. Review Secure Configuration Documents adopting best practices for servers OS, Web application, Database, Security Devices, Network Devices, Desktops, Laptops, Mobile devices etc. 3.5. Review of Network Security including	Progress report as mutually agreed. Recommend and incorporate Changes to Existing Information Security Policies, Procedures. Prepare new procedures and guidelines as per gaps. Detailed report with recommendations and action plan for the IT department for coordination and reporting mechanism (Dashboard etc.) to CISO.	**10 Weeks from the Date of Purchase Order**

various wireless technologies, Security Design, Access Control, etc. 3.6. Review of the existing network topology/ Network Security Architecture and deployment of the security controls within the organization like firewalls, IDS/IPS, network segmentation, Web Gateway, Mail Gateway, Proxy, DLP, Patch Management, AV, SIEM, etc. 3.6.1. Firewall – • Rule/ ACL/NAT base audit 3.6.2. IPS/IDS – • Assessment of Signature applied / Available. • Review protection against the latest vulnerabilities and blended attacks. • Review on threat detection 3.6.3. Web Gateways – • Access and Policy review. • URL and Content filtering review • Review on hits for riskiest and blocked URL 3.6.4. Mail Gateways – • Spam, Content and Malware policy review • Review on threat detection 3.6.5. Proxy – • Review ACL / policies 3.6.6. DLP – • Review of Classification of Unstructed Data. • Review Policies (Data at Rest, In-motion and at endpoint)	Document on best suitable proposed Architecture Presentation with proof of working model. Document on the comparison/analysis made and the solutions identified. Anything else as mutually agreed upon.	

• Review health status of endpoint systems and Servers • Review of deployment status 3.6.8. AV – • Review of Virus detection, location-wise, threat-wise. • Review of Deployment status 3.6.9. SIEM– • Review of alerts/ rules (Co-relation rules enabled) • Scope and architecture • Incident Management process 3.7. The bidder would identify network and design architectural weaknesses in term of security, performance, scalability, etc. 3.8. Review of Information / Cyber Security Incident response mechanism. 3.9. Review and prepare Information / Cyber Security Metrics alongwith Benchmarks 3.10. Preparation of RACI matrix for the Information Security Functions and Activities. 3.11. The bidder shall provide recommendations to increase the effectiveness of the security controls. 3.12. The bidder would review advanced real time vulnerability and threat intelligence including Anti-Phishing, Anti- Trojan, and Anti- Malware services, Zero Day		

vulnerabilities, Advanced persistence threat, etc. and specific actionable/ recommendations as per Bank existing / proposed technology environment. 3.13. The bidder shall arrive at the methodology using globally acceptable standards and best practices, suitable for the Bank, after taking into consideration the effort estimate for completion of the same and the resource and the equipment requirements. 3.14. Knowledge Transfer during execution of the Assignment, provide documentation and material. 3.15. Assess & Develop IS performance dashboard focused on ROI with a mechanism and process to convey value of investment on IS infrastructure across the Bank including Top Management using industry standard Benchmark. 3.16. The bidder would recommend improvements to better align the security architecture with business objectives, the Bank's information security policy and industry best practices. 3.17. Assisting Bank in preparation, evaluation, selection, implementation and monitoring of various IS Tools applications etc. 3.18. Conduct gap analysis for the security technologies and architecture 3.19. Review of preparedness in the Bank vis-à-vis advisory from NCIIPC/ CERT-In / GoI / IT Act. etc.	Document on best suitable proposed Architecture Presentation with proof of working model. Document on The comparison / analysis made and the solutions identified. Anything else as mutually agreed upon.	

4.0 Setting up of SOC The requirement study of the Bank current IT and IS Infrastructure and proposal for the resilience structure and framework for operationalization of CSOC and its set-up	Requirement study for setting-up of CSOC, Preparation of RFP, Monitoring and implementation of CSOC related guidelines of CSITE, RBI, incident reporting set-up by keeping a provision for creation of dashboard system of security incidents and its reporting to the concerned forum viz. CSITE, RBI, NCIIPC, CERT-IN.	**10-15 weeks from placement of work order**

Note: The circulars/advisories issued by RBI towards Cyber Security are given at the end of this RFP document and bidders have to take into account these advisories while executing the activities. The copies of advisories shall be provided to the bidders in physical copy (if required) at the time of attending pre-bid meeting. The bidder also have to take into account other guidelines on Cyber Security issued by RBI till the date of this RFP and issued during the execution of this project.

Bidder shall monitor progress of all the activities specified in the scope of work and submit free of cost periodic progress report about various aspect of the study to the Bank. The Bank on mutual agreement between both Parties may change the periodicity of such reports. Extracts of the progress report to be termed as "Executive Summary" shall be submitted in 3 copies, along with 3 copies of monthly progress report.

Also the successful Bidder will have to participate in periodic meetings with the Bank to discuss project progress and various issues concerning efficient and timely execution. If at any time it should appear to the Bank that the actual progress of work does not conform to the approved milestones, the Bidder shall produce at the request of the Bank a revised timeline showing the modification to the approved timelines necessary to ensure completion of the works within the time for completion.

The submission to an approval by the Bank of such timeline as the furnishing of such particulars shall not relieve the Bidder of any of his duties, obligations or responsibilities under the Contract.

In case during execution of works/Services the progress falls behind schedule then the Bidder should notify the Bank in writing about the same with proper causes for the delay and recovery procedures mentioned. Bidder shall deploy extra manpower, resources to make up the progress. The plan for deployment of extra man power/ resources will be submitted to the Bank for its review and approval. All time and cost effect in this respect shall be borne by the Bidder.

6. Period of Contract:

The contract will be valid from commencement of contract and upto one year from the date of implementation of project. Bank will enter into a service contract with successful bidder for a period of 1 year from the date of implementation of project.

Date of implementation of project shall be date of acceptance of the letter of award (Starting Date) or such other date as may be fixed by NHB. The same date shall be considered for renewal of services etc., if applicable

Note:

This RFP is not exhaustive in describing the functions, activities, responsibilities and services for which the consultants will be responsible. The Bidder, by participation in this tender, implicitly confirm that if any functions, activities, responsibilities or services not specifically described in this RFP are necessary or appropriate for the proper performance and required for compliance of Statutory or Regulatory compliance and they will be deemed to be implied by and included within the scope of services under this RFP at no extra cost and Bidder's response to the same extent and in the same manner as if specifically described in this RFP and Bidder's response.

7. Instructions to Bidders

7.1 General :-

The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding documents. Failure to furnish all information required by the Bidding/Tender/RFP documents may result in the rejection of its Bid and will be at the Bidder's own risk.

- All costs and expenses incurred by the Bidders in any way associated with the development, preparation, and submission of responses, including but not limited to; the

attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by NHB, will be borne entirely and exclusively by the Bidder.

- No binding legal relationship will exist between any of the Bidders and NHB until execution of a contractual agreement, except the pre-contract integrity pact to be submitted along with the Bid. Post evaluation and finalization of the Bids and identification of the successful Bidder, the integrity pact will for part of the definitive agreement to be signed by the successful Bidder. For the other Bidders, the pre-contract integrity pact will be binding on them for any acts/omissions committed by the Bidder in violation/breach of the said pre-contract integrity pact in relation to the Bid submitted.

- Each Bidder acknowledges and accepts that NHB may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Consultant (s).

- Every Bidder will, by submitting his Bid in response to this RFP, be deemed to have accepted the terms of this RFP and the Disclaimer.

- Bidders are required to direct all communications related to this RFP, through the nominated Point of Contact persons, mentioned below:

Amit Sinha Asst. General Manager, National Housing Bank , All Audits Department Head Office Core 5-A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi – 110003 Phone No : 011-39187122 Email : amit.sinha@nhb.org.in	Prabhat Ranjan Deputy Manager, National Housing Bank, All Audits Department Head Office Core 5-A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi – 110003 Phone No : 011-39187160 Email: prabhat.ranjan@nhb.org.in

- NHB may, in its absolute discretion, seek additional information or material from any Bidder/s even after the tender/RFP closes and all such information and material provided must be taken to form part of that Bidder's response.

- Bidders should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RFP could be conveyed promptly.

- If NHB, in its absolute discretion, deems that the originator of any query will gain an advantage by any response to such query, then NHB reserves the right to communicate such response to all Bidders.

- Queries / Clarification if any, may be taken up with the contact person/s detailed above before the deadline for submission of Bids between 11 am to 0530 pm on Monday to Friday, excluding public holidays.

- Bidder should not have been blacklisted/debarred from participation in the Bid process by any of the Govt. Departments/PSUs/Banks/Financial Institutes in India.

- NHB will notify all short-listed Bidders in writing or by mail or by publishing in its website as soon as practicable about the outcome of their RFP. NHB is not obliged to provide any reasons for any such acceptance or rejection.

- NHB reserves the right to cancel the entire tendering process at any point of time prior to award of contract if deemed fit.

7.2 Pre-Bid Meeting

For the purpose of clarification of doubts of the Bidders on issues related to this tender/RFP, NHB intends to hold a Pre-Bid meeting on the date and time as indicated in the RFP. The queries of all the Bidders, in writing, should reach by e-mail or by post on or before 04.10.2019 by 15:00 Hrs on the address/email as mentioned on page 05 of this RFP. It may be noted that no queries of any Bidder shall be entertained received after the Pre-Bid meeting. Clarifications on queries will be given in the Pre-Bid meeting. Only the authorized representatives of the Bidders, will be allowed to attend the Pre-Bid meeting.

7.3 Soft Copy of Tender/RFP Document

The soft copy of the Tender/RFP document will be made available on NHB's website http://www.nhb.org.in . The Bidders will need to pay the non-refundable fee of Rs. 10,000/- (Rupees Ten Thousand only) by way of ECS into NHB' account as described in Clause **7.12(i).**

The proof of the payment should be enclosed and put in the envelope containing the Technical Bid; in the absence of which the Bid may not be considered for further evaluation.

7.4 Non-Transferability of Tender/RFP

This tender/RFP document is not transferable.

7.5 Erasures or Alterations

The offers containing erasures or alterations may not be considered. Any interlineations', erasures or overwriting in technical Bids may be considered at the discretion of NHB only if they are initialed by the person signing the Bids. However, any interlineations', erasures or overwriting in any form will not be accepted in the commercial Bid. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "as given in brochure/manual" is not acceptable. However, NHB may treat offers not adhering to these guidelines as unacceptable. NHB may, in its absolute discretion, waive any minor non-conformity or any minor irregularity in the offer. This shall be binding on all Bidders and NHB reserves the right for such waivers.

7.6 Amendment to the Bidding/Tender/RFP document

- At any time prior to the deadline for submission of Bids, NHB, for any reason, may modify the Bidding/Tender/RFP Document, by amendment.
- The amendment will be posted on NHB's website www.nhb.org.in
- All Bidders must ensure that all amendments/enhancements (if any) in the RFP have been considered by them before submitting the Bid. NHB will not have any responsibility in case some omission is done by any Bidder.
- NHB at its discretion may extend the deadline for the submission of Bids.
- NHB shall not be liable for any communication gap. Further NHB reserve the right to scrap the tender or drop the tendering process at any stage without assigning any reason.

7.7 Language of Bid

The Bid prepared by the Bidders, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and NHB and supporting documents and printed literature shall be written in English.

7.8 Masked Commercial Bid

The Bidder should submit a copy of the actual price Bid (as per the format specified by NHB being submitted to NHB separately by masking the actual prices. **This is mandatory**. The Bid may be disqualified if it is not submitted by masking it properly. NHB reserves the right to cancel the Bid/tender process at the time of commercial evaluation, if the format/detail (except price) of 'Masked Commercial Bid' does not match with the format/detail of actual Commercial Bid submitted.

7.9 Right to Alter Location / Quantities

NHB reserves the right to alter the proposed location/s specified in the RFP. NHB also reserves the right to add/delete one or more location/s from the list specified in this RFP, from time to time.

7.10 Documents Comprising the Bid

1. Bidder's information in the format as prescribed in **Annexure I;**
2. Bidder's Experience details in the format as prescribed in **Annexure II;**
3. Compliance Statement Declaration in the format as prescribed in **Annexure III;**
4. List of Deviations, if any, in the format as prescribed in **Annexure IV;**
5. Information on Minimum Eligibility in the format as prescribed in **Annexure V:**
6. **The Technical Proposal**: The Technical Bid should be submitted in the format as prescribed in **Annexure VII** along with the covering letter in the format as prescribed in **Annexure VI**. Annexure I, II , III, IV, V , VI, VII, X ,XI,XII,XIII,XIV must be submitted along with Technical Proposals.
7. The **Commercial Proposal**: The Commercial Bid should be submitted in the format as prescribed in **Annexure IX** along with the covering letter in the format as prescribed in **Annexure VIII**.
8. ECS Mandate in the format as prescribed in **Annexure X;**
9. Letter of Competency in the format as prescribed in **Annexure XI;**
10. Curriculum Vitae (CV) of the Key Personnel in the format in **Annexure XII;**
11. Escalation Matrix in the format in **Annexure XIII;**
12. Pre-Contract Integrity Pact (wherever applicable) in the format in **Annexure XIV** *(The Pre-Contract Integrity Pact should be submitted neatly typed in on Rs.100/- non-judicial stamp paper duly signed by the authorized signatory and the same will be signed on behalf of NHB subsequently. The date of execution should be the date as mentioned in the Technical Bid by the Bidder)*
13. Service Level Agreement as per format given in **Annexure XV**
14. Non Disclosure Agreement as per format given in **Annexure XVI**
15. Performance Bank Guarantee as per format given in **Annexure XVII**

Note: Bids without the RFP cost and EMD amount will be rejected.

7.11 Bid Currency

i. Bids to be quoted in Indian Rupee only.

7.12 Earnest Money Deposit (EMD)

i. All the responses must be accompanied by a refundable interest free security deposit of Rs. One Lac only (Rs. 1,00,000/- only), by way of an e-payment in favour of **National Housing Bank**. The Accounts details are given below:

S.No	Type	Beneficiary Particulars
1	Name	National Housing Bank
2	Address	Core 5A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi 110 003
3	Bank Name	State Bank of India
4	Bank Branch Address	Pragati vihar Delhi Branch, Ground Floor, Core-6, Scope Complex, Lodhi Road, New Delhi – 110 003
5	Type of Bank Account	Current account
6	Bank A/C No	52142903844
7	IFCS code of Bank branch	**SBIN0020511**
8	MICR No	**110002658**

ii. The proof of the EMD payment and Cost of RFP should be enclosed and put in the envelope containing the Technical Bid; in the absence of which the Bid may not be considered for further evaluation. The Bidders are also required to submit ECS Mandate Form as enclosed in **Annexure-X**.

iii. Any Bid received without EMD in proper form and manner shall be considered unresponsive and rejected.

iv. Request for exemption from EMD will not be entertained.

v. Save as otherwise provided herein or in the definitive agreement, the EMD amount of all unsuccessful Bidders would be refunded on completion of the tendering process.

vi. The EMD security may be forfeited:

- If a Bidder withdraws its Bids during the period of Bid validity;
- If a Bidder makes any statement or encloses any form which turns out to be false/incorrect at any time prior to signing of the contract;
- In case of successful Bidder, if the Bidder fails to Sign the contract; and
- In case of any breach of the pre-contract integrity pact.

7.13 Implementation schedule

- The selected vendor will be required to report at the NHB Head Office for commencement of the services within 10 days of acceptance of work order.

- The Bidder shall be responsible for delivery of the services.

S.No	Event	Delivery Schedule (From date of acceptance of work order/letter of award)
1.	Kick off meeting	7 days
2.	Commencement of services	7-10 days

- Billing cycle will commence only after execution of SLA as per terms of the RFP.

7.14 Performance Bank Guarantee (PBG)

The selected Bidder will be required to provide a 25 % of the total cost of contract value, in the form of bank guarantee from a scheduled commercial bank in the format as substantially prescribed in **Annexure-XVII**. Contract value for this will be X {X is Charges towards Cyber Security Framework preparation (as quoted in Commercial Bid i.e. Annexure IX) }. The PBG should be valid till at least 06 months beyond the expiry of contract period or such other extended period as NHB may decide. The PBG is required to protect the interest of NHB against the risk of non-performance or default in RFP Term/s, including non-compliance of applicable statutory provisions including labour laws and any other laws/rules/regulations, by the successful Bidder. Default in successful implementation of the conditions of the contract, may warrant the invoking of PBG, and also if any act of the Consultants /Bidder results into imposition of Liquidated Damages/penalty, then NHB reserves the right to invoke the Performance Bank Guarantee submitted by such Bidder. The decision of NHB as to non-performance or default in RFP Term/s, including non-compliance of applicable statutory provisions etc shall be final and binding on the successful Bidder.

7.15 Period of Validity of Bids

- Prices and other terms offered by Bidders must be valid for an acceptance period of six months from the date of opening of commercial Bid.

- In exceptional circumstances NHB may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing. The Bid security provided shall also be extended.

7.16 Format and Signing of Bids

Each Bid shall be submitted in two parts:

- **Part I**: consists of Minimum Eligibility Criteria, Technical Bid and Masked Commercial Bid [price Bids without any price]. The above contents will be referred to as **"Technical Proposal".**

- **Part II** : covering only the Commercial Bid herein referred to as "**Commercial Proposal"**

- The Original Bids shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the contract. The person or persons signing the Bids shall put their initials on all pages of the Bids, except for un-amended printed literature.

7.17 Sealing and Marking of Bids

- The non-window and sealed envelope containing both Part I ad Part II as described in 8.16 super scribing **" Proposal for Appointment of Cyber Security Consultant in National Housing Bank"** shall be addressed to NHB at the address given below:

  Deputy General Manager,
  All Audits Department,
  National Housing Bank
  Core 5A, 4th Floor, India Habitat Centre
  Lodhi Road, New Delhi – 110003

- All envelopes should indicate on the cover the name and address of Bidder along with contact number and email address.

- The Bidder shall seal the envelopes containing Technical and Commercial proposals separately.

- The envelope should be non-window and separately super scribed as **"Technical Proposal for Appointment of Cyber Security Consultant in National Housing Bank "**, and **"Commercial Proposal for Cyber Security Consultant in National Housing Bank "**, as applicable.

- If the envelop is not sealed and marked, NHB will assume no responsibility for the Bid's misplacement or its premature opening.

- Bids not sealed properly shall not considered and will stand rejected without recourse.

7.18 Deadline for submission of Bids

- The Bids must be received by NHB at the addressed specified, not later than the last date of Bid submission as indicated above.

- In the event of the specified date for the submission of Bids, being declared a holiday for NHB, the Bids will be received up to the appointed time on the next working day.

  NHB may, at its discretion, extend the deadline for submission of Bids by amending the Bid documents with intimation on NHB's website, in which case, all rights and obligations

of NHB and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

7.19 Late Bids

Any Bid received by NHB after the deadline for submission of Bids prescribed by NHB will be rejected and returned unopened to the Bidder.

7.20 Opening of Bids by NHB

- On the scheduled date and time, Bids will be opened by NHB Committee in presence of Bidder representatives who will attend the meeting on the specified date and time.
- **Place of Opening of Technical Bids:**

  National Housing Bank
  Core 5A, 3rd – 5th Floor, India Habitat Centre
  Lodhi Road, New Delhi – 110003

- The Bidder name and presence or absence of requisite EMD, RFP cost and such other details as NHB, at its discretion may consider appropriate, will be announced at the time of Technical Bid opening.

7.21 Clarification of Bids

During evaluation of Bids, NHB, at its discretion, may ask the Bidder for clarification of its Bid. The request for clarification and the response shall be in writing (Fax/e-Mail), and no change in the substance of the Bid shall be sought, offered or permitted.

7.22 Preliminary Examinations

- NHB will examine the Bids to determine whether they are complete, the documents have been properly signed; supporting papers/documents attached and the Bids are generally in order etc.
- NHB may, at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

- The decision of NHB is final towards evaluation of the Bid documents.

7.23 Proposal Ownership

The proposal and all supporting documentation submitted by the Bidder shall become the property of NHB unless NHB agrees to the Bidder's specific request/s, in writing that the proposal and documentation be returned or destroyed.

7.24 Instructions to the Bidders

The Bidder shall not outsource the work assigned by NHB, to any third party except with NHB's prior written consent and attend all complaints registered by NHB through its own service/support infrastructure only.

7.25 Price Composition & Variation

- The Bidder should clearly furnish the cost matrix strictly as per the structure, if any, provided in the **Annexure IX**. Any deviation may lead to Bid rejection. Also no options should be quoted other than as per the commercial Bid. Wherever options are given, the Bid is liable to be rejected.
- The commercial offer shall be on a fixed price basis. No price variation relating to cost of Cyber Security Framework preparation excl. taxes (present and future) will be entertained for any work assigned during the period of contract.
- Only Statutory taxes/cess/charges will be paid as actual as per statutory revision.
- Date of implementation of project shall be date of acceptance of the letter of award (Starting Date) or such other date as may be fixed by NHB. The same date shall be considered for renewal of services etc., if applicable.

7.26 Timely availability of Support Services

- The Consultant should have proper and adequate support mechanism in place at New Delhi and Mumbai to provide all necessary support under this project.

7.27 Manuals/Documents

The Consultant shall provide required documentation/s for the services supplied during the period of contract as also required documentation of knowledge transfer.

7.28 Modification and Withdrawal

- Every Bidder shall submit only one proposal. If any Bidder submits more than one proposal, all such proposals shall be disqualified.
- The Bidders are advised to submit the Bids only after the Pre-Bid Meeting as the Bids once submitted will be treated, as final and no further correspondence will be entertained on this. No Bid will be allowed to 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.
- NHB has the right to reject any or all Bids received without assigning any reason whatsoever. NHB shall not be responsible for non-receipt / non- delivery of the Bid documents due to any reason whatsoever.

7.29 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 commercial Bid. Failure to do so will make the Bid liable to be rejected.

7.30 Terms and Conditions of the Bidding firms

The Bidding firms are not required to impose their own terms and conditions to the Bid and if submitted will not be considered as forming part of their Bids. The Bidders are advised to clearly specify the deviations as per Annexure-IV, in case terms and conditions of the contract applicable to this RFP are not acceptable to them. The Bidders should also describe clearly in what respect and up to what extent the equipment and services being offered differ/ deviate from the specifications laid down in the specifications and requirements.

7.31 Local conditions

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

7.32 Contacting NHB or putting outside influence

Bidders are forbidden to contact NHB 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.

7.33 Proposal Content

The Bidders' proposals are central to the evaluation and selection process. Therefore, it is important that the Bidders carefully prepare the proposal. The quality of the Bidder's

proposal will be viewed as an indicator of the Bidder's capability to provide the solution and Bidder's interest in the project.

7.34 Banned or Delisted Bidder

Bidders have to give a declaration that they have not been banned or delisted by any Government, Quasi Government agencies, PSUs or PSBs and its subsidiaries. If a Bidder has been banned by any Government, Quasi Government agencies, PSUs or PSBs and its subsidiaries, this fact must be clearly stated .If this declaration is not given, the Bid will be rejected as non-responsive. This declaration will be submitted along with the Technical Bid.

7.35 Compliance with Laws

(a) The Consultant shall undertake to observe, adhere to, abide by, comply with and notify NHB about all laws in force or as are made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this tender and shall indemnify, keep indemnified, hold harmless, defend and protect NHB and its employees/officers/staff/ personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

(b) The Consultant shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc, as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NHB and its employees/ officers/ staff/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and NHB shall give notice of any such claim or demand of liability within reasonable time to the Consultant.

(c) In case NHB undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights of the Consultant under this Contract.

7.36 Intellectual Property Rights

The Bidder warrants that in the event of its selection as the Cyber Security Framework implementation firm: -

(a) The Inputs to be provided by it shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.

(b) It further warrants that the Deliverables shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.

(c) In the event that the Deliverables become the subject of a claim of violation or infringement of a third party's intellectual property rights, the Bidder shall, at its choice and expense: (a) procure for NHB the right to continue to use such Deliverables; (b) replace or modify such Deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified Deliverables as the infringing Deliverables; or (c) if the rights to use cannot be procured or the Deliverables cannot be replaced or modified, accept the return of the Deliverables and reimburse NHB for any amounts paid to the Bidder for such Deliverables, along with the replacement costs incurred by NHB for procuring an equivalent equipment in addition to the penalties levied by NHB . However, NHB shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the Bidder shall be responsible for payment of penalties in case service levels are not met because of inability of NHB to use the proposed solution.

(d) The indemnification obligations stated in this clause apply only in the event that the Indemnified Party provides the Indemnifying Party prompt written notice of such claims; grants the Indemnifying Party sole authority to defend, manage, negotiate or settle such claims; and makes available all reasonable assistance in defending the claims (at the expense of the Indemnifying Party). Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the Indemnified Party make any payment or bear any other substantive obligation without the prior written consent of the Indemnified Party. The indemnification obligations stated in this clause reflect the entire liability of the parties for the matters addressed thereby.

(e) The Bidder acknowledges that business logics, work flows, delegation and decision making processes of NHB are of business sensitive nature and hence shall not be referred to other clients, agents or distributors of the software. The project shall be deemed as incomplete in case the desired objectives of the project as mentioned in the scope of the project are not met and in case the system is unable to facilitate the processes duly supported by various requirements as envisaged in the RFP.

7.37 False / Incomplete statement

Any statement/declaration made by the Bidder, if proved wrong or false or incomplete or such as to withhold any information relevant to the award of the tender, at any stage of the tender/Bid process or in the event of his Bid/tender having been accepted at any stage of the contract, shall render his/their Bid(s)/tender(s)/contract(s) liable to be cancelled/rescinded, in addition to the followings:

a. If such statement is found at the tender stage, his total earnest money shall be forfeited and tender will be summarily rejected.
b. b. In case such a statement is found at the contract stage appropriate action as decided by NHB shall be applicable.

9. Bids (Technical & Commercial) and Bid Evaluation Methodology

i. Bid Evaluation Methodology

Introduction

a. To meet the Bank's requirements, as spelt out in the RFP, the selected Bidder must have the requisite experience in providing services in the field of Cyber Security Framework that would be required to successfully provide the services sought by the Bank, for the entire period of the contract. The evaluation process of the bids proposed to be adopted by the Bank is indicated below. The purpose of it is only to provide the Bidder an idea of the evaluation process that the Bank may adopt. The Bank reserves the right to modify the evaluation process at any time during the Tender process (before submission of technical and commercial responses by the prospective bidder), without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change. Any time during the process of evaluation the Bank may seek specific clarifications from any or all the Bidder.
b. It **may please be noted that the Bank reserves the right to reject any proposal in case same is found incomplete or not submitted in the specified format given in this RFP document**.
c. The details of 'Minimum Eligibility Criteria', provided by the bidder in its response to this RFP, will be evaluated first, based on the criteria described in section**.** The technical and commercial responses to this RFP will be considered further only for those bidders who meet the **Minimum Eligibility Criteria**.

ii. The technical and commercial response evaluation will be based on the criteria described in following section onwards.

a. Minimum Eligibility Criteria

S No	Criteria
1.	The Bidder must be an ISO 27001 certified organization and should be a Private Limited of Limited Company
2.	During last five years (i.e. between 01.4.2014 to 31.03.2019) the Bidder should have carried out the work of implementation of cyber security framework in at least one SCB/ All India FI, having asset size of more than Rs. 1000 Crore as on March 31, 2019).
3.	The Bidder must be empanelled with CERT-In as Information Security Audit Organization
4.	The bidder Company should have at-least 25 qualified Information Security / Cyber Security professionals (DISA/CISA/CISM/CDAC/ CEH) in their payroll.
5.	The Bidder should have its own office in Delhi NCR and Mumbai Metropolitan Region (MMR).
6.	The Bidder firms should not have been black listed/ debarred by any Government Financial Institutions /Banks/ RBI/ ICAI/ IBA / Government / Semi Government Departments/ PSUs / in India during last 5 years and Blacklisting should not be in force.
7.	The Bidder should not be owned or controlled by any Director or Employee of National Housing Bank, both present and those who have retired in the last two Years, or by any of their Relatives. Further, the Bidder shall not engage any of the foregoing persons as partners, employees or contractors for any work whether connected with the "Assignment/ Job/ Engagement" nor shall they benefit directly or indirectly from the "Assignment/ Job/ Engagement" in any manner.
8.	Average annual professional income from information / cyber security activities of the firm during last three years i.e. 2016-17, 2017-18 & 2018-19 should be minimum Rs. 10 Crore.

A. Bidder should submit documentary evidence (acceptable to the Bank) of the Information given in the related formats in respect of all above mentioned criteria while submitting the proposal. Proposal of bidder who do not fulfill the above criteria or who fail to submit documentary evidence to the satisfaction of the Bank would be rejected.

B. Bidders fulfilling the Minimum Eligibility Criteria will only be considered for further technical evaluation.

i. Technical bids received from the Bidder will be opened at the scheduled time in the presence of available bidders.

b. The technical bid will be analyzed and evaluated, based on which the Technical Score (TS) shall be assigned to each bid. The mark distribution criteria of the Technical evaluation are as follows:

Mark Distributions (Maximum Points 100)

S No	Details	Marks
	Part I	
1.	Existence of the firm in the field of providing Information Security / Cyber Security Services (Max Marks 15) More than 15 Years More than 10 but ≤ 15 Years More than 05 but ≤ 10 Years	 15 10 05
2.	The number of professional staff (excluding typists, stenographers, computer operators, secretary/ies and subordinate staff etc.) in the area of Information Security / Cyber Security (Bidder will provide a list of staff signed by authorized signatory on their letter head which will include Qualification, designation, No of year of Experience etc.) (Max Marks: 15) More than 75 More than 40 but ≤ 75 More than 25 but ≤ 40	 15 10 05
3.	No. of SCBs/All India FIs/ PSBs, where the vendor has carried out implementation of Cyber Security Framework	

	More than 5 More than 3 but ≤ 5 More than 1 but ≤ 3	15 10 05
4.	No of satisfactory service certificate issued by client pertaining to implementation of Cyber Security Framework More than 5 More than 3 but ≤ 5 More than 1 but ≤ 3	 15 10 05
5.	Average annual professional income of the firm (From IT/ Cyber Security) during last three years i.e. 2016-17, 2017-18 and 2018-19 (Max Marks: 15) More than 20 Crore More than 15 but ≤ 20 Crore More than 10 but ≤ 15 Crore	 15 10 05
Part II		
6.	Presentation on proposed roadmap for implementation of Cyber Security Framework and setting-up of C-SOC	25

ii. Bidders have to provide certified copies of supporting documents against each criteria mentioned above, without which bid may be rejected.

iii. The minimum qualification score for the Technical Bids would be 70 (cut-off marks) out of Total 100 marks (Including marks for presentation).

iii. Financial Bid

i. Only firms successfully qualifying the requisite criteria of the Technical Bid process shall be considered eligible for the Financial Bid Round. The evaluation of the Financial Bids would be as follows:

ii. The lowest bid shall be assigned the maximum Financial Score of 100 points.

iii. The Financial Scores of the other Financial Bids will be computed relative to the lowest evaluated Financial Bid.

iv. The Financial Score computing methodology is as follows:

- Financial Score (Bid under consideration) = $\frac{\text{100x Price of the lowest bid}}{\text{Price of the bid under consideration}}$

v. Final Processing

- Proposals would be ranked according to their Final Score arrived at by combining Technical and Financial Scores as follows:
  Final Score = Technical Score x T + Financial Score x F
  (T - Weightage given to the Technical Bid, F - Weightage given to the Financial Bid,
  T + F = 1)
  Weightage for the bids are as follows:

Technical Bid T	60%
Financial Bid F	40%
Total Weightage	100%

The firm achieving the highest combined Technical and Financial Score will be invited for negotiations.

The Bank reserves the right to revise the evaluation criteria, methodology, distribution points and weight age; if it finds it necessary.

10. Commercial Terms and Conditions

Bidders are requested to note following commercial terms and conditions for this project.

10.1 Currency

The Bidder is requested to quote in Indian Rupees ('INR'). Bids in currencies other than INR may not be considered.

10.2 Price

a) The Price quoted by the Bidder should include all type of costs.
b) The price should be valid and firm for full contract period.
c) The price should be inclusive of all taxes (except GST), duties, levies charges, transportation, insurance, as per Commercial Bid.
d) The price quoted by the Bidder shall remain firm during the Bidder's performance of the contract

e) Bid submitted with adjustable price quotation will be treated as non-responsive and will be rejected.
f) Bid submitted with adjustable price quotation will be treated as non-responsive and will be rejected.

10.3 Payment Terms

Any payment will be released only after submission of PBG & post-signing of SLA & NDA as per the following payment terms.

The service provider shall be paid as under:

- 25% of the contract value on commencement of project
- 35% of the contract value on submission of Cyber Security Policy & Cyber Crisis Management Plan and after its acceptance by the Bank
- 40% of the contract value on completion of the project and final sign-off

10.4 Payment in case of termination of contract

The entire contract is to be completed in full and any prior termination / inability to complete the project by the bidder shall result in no payment and forfeiture of EMD submitted by the bidder. No request for pro-rata payment shall be entertained by the Bank.

11. General Terms and Conditions

11.1 The Bidder is expected to peruse all instructions, forms, terms and specifications in this RFP and its Annexures. Failure to furnish all information required in the RFP Documents, in the formats prescribed or submission of a proposal not substantially responsive or submission of unnecessary additional information as part of response to this RFP Document may result in rejection of the proposal.

11.2 All such amendments made by NHB to the RFP shall become part and parcel of the RFP and same will be notified on NHB's website. The Bidders are required to have a watch on NHB's website for any such amendment.

11.3 Bidders must take into consideration each and every line of this RFP document while preparing technical and commercial proposal for the project. Bidders are requested to get any issue clarified by NHB before submitting the responses/Bids. The Bids submitted should be complete in all respect meeting all deliverables under the project. It will be the sole responsibility of the successful Bidder to deliver each and everything as per the

scope of the work during the contracted period. NHB will not be responsible in case of any requirement is underestimated or any requirement is not interpreted in right perspective.

11.4 NHB reserves the right to change the requirement specifications and ask for the revised Bids or the tendering process without assigning any reasons.

11.5 NHB shall be under no obligation to accept the lowest or any other offer/Bid received in response to this RFP and shall be entitled to reject any or all offers including those received late or incomplete offers, without assigning any reason whatsoever. NHB reserves the right to make any changes in the terms and conditions of contract. NHB will not be obliged to meet and have discussions with any Bidder, and or to consider any representations. NHB reserves the right to accept or reject, fully or partially, any or all offers without assigning any reason. The decision of NHB in this regard is final and no further correspondence in this regard will be entertained.

11.6 Although service window is **1000 Hrs to 1800 Hrs**, the selected Bidder must provide services beyond the above time in case of urgent requirement of NHB without any extra cost.

11.7 Notwithstanding anything to the contrary contained in the contract, NHB shall be at liberty to invoke the Performance Bank Guarantee in addition to other remedies available to it under the contract or otherwise if the successful Bidder fails to fulfill any of the terms of contract / order or commits breach of any terms and conditions of the contract.

11.8 On faithful and satisfactory execution of assignments under the contract in all respects, the PBG of the successful Bidder will be released by NHB, if not forfeited due to any reason as provided herein, after a period of 100 days after completion/execution of the assignments/contract.

11.9 Bidder must deploy manpower having requisite qualification, experience, skill-set etc. for the project/contract.

11.10 NHB reserves the right to call for any additional information and also reserves the right to reject the proposal of any Bidder if in the opinion of NHB, the information furnished is incomplete or the Bidder does not qualify for the contract.

11.11 The scope of the proposal shall be on the basis of single point responsibility, completely covering the products and services specified under this RFP, on end-to-end solution basis.

11.12 The Commercial and Technical Bids will have to be signed on all pages of the Bid by the authorized signatory. Unsigned Bids would be treated as incomplete and would be rejected.

11.13 By submitting proposal/bid, the Bidder agrees to promptly execute contract with NHB for any work awarded to the Bidder. Failure on the part of the awarded Bidder to execute a valid contract/service level agreement with NHB, will relieve NHB of any obligation to the Bidder, and a different Bidder may be selected.

11.14 Time and quality of the service are the essence of this agreement/contract. Failure to adhere to the same will be considered as breach of the terms and conditions of the contract.

11.15 Penalty

The Bank expects basic service level from the firm.

The selected bidder will have to complete the project within stipulated time-frame indicated in scope of work (clause 5).

In case the firm fails to comply with the requirement given in clause no 5 or delays the project by more than a month's time, a penalty of upto one percent of contract value per day delay may be charged by the Bank, up to a maximum of 20% of the project cost. In case the delay is more than 30 days, the Bank reserves the right to terminate the contract and also forfeit the EMD amount deposited by the firm.

11.16 Removal and/or Replacement of Personnel

a) If, for any reason beyond the reasonable control of the the firm, it becomes necessary to replace any of the Key Personnel (personnel according to NHB engaged for key assignments under the contract by the firm), the firm shall forthwith provide as a replacement a person of equivalent or better qualifications and skills.

b) If NHB finds that any of the Personnel have (i) committed serious misconduct or has been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the firm shall, at NHB's written request specifying the grounds therefore, forthwith provide as a replacement a person with qualifications and experience acceptable to NHB.

c) For any of the Personnel provided as a replacement under Clauses (i) and (ii) above, the contract value shall not change, (i) the firm shall bear all additional travel and other costs

arising out of or incidental to any removal and/or replacement, and (ii) the total contract value shall not exceed the amount quoted in financial bid.

11.17 Acceptance of Work Order/Letter of Award

NHB will notify the successful Bidder in writing by issuing a letter of award/work order in duplicate. The successful Bidder has to return the duplicate copy to NHB within 7 working days from the date of the letter of award/work order duly accepted, and signed by Authorized Signatory in token of acceptance. However, NHB has a right to cancel the letter of award/work order, if the same is not accepted within the stipulated period.

11.18 Definitive Agreement

The successful Bidder will sign Service Level Agreement (SLA) substantially in the format as provided in **Annexure XV** and the Confidentiality cum Non-Disclosure Agreement (NDA) in **Annexure XVI** with NHB within 15 days of the letter of award (LoA) or within such extended period as may be decided by NHB. All expenses, stamp duty and other charges/ expenses in connection with the execution of the Agreement/s as a result of this RFP process shall be borne by successful Bidder. Copy of Board resolution or power of attorney showing that the signatory has been duly authorized to sign the acceptance letter, contract and non-disclosure agreement, should be submitted.

11.19 Taxes

Only Statutory taxes/cess/levies will be paid by NHB on actual basis as per statutory rates prevalent during the period of service provided. All other charges as applicable will be borne by the Bidder. NHB is authorized to make such tax deduction at source as may be necessary as per law/rules in force in respect of payments made to the Consultants.

11.20 Liquidated Damages

If the consultant fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the final contract negotiations, NHB reserves the right to recover damages maximum of Bank Guarantee Value for non-performance/delayed performance as and by way of liquidated damages from the applicable payments consolidated on quarterly basis.

11.21 Use of Contract Documents and Information

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

11.22 Assignment

The successful bidder shall not assign/subcontract, in whole or in part, its obligations to perform under the contract, except with NHB's prior written consent.

11.23 Duration of Contract

The contract will be valid from commencement of contract and upto one year from the date of implementation of project. Bank will enter into a service level agreement with successful bidder for the said period.

11.24 Pre-Contract Integrity Pact Clause (To be included as and when required on case to case basis)

An "Pre-Contract Integrity Pact" would be signed between NHB and the Bidder. This is a binding agreement between NHB and Bidders. Under this Pact, the Bidders agree with the Buyer to carry out the assignment in a specified manner. The format of Pre-Contract Integrity Pact will be as per **Annexure - XIV**.

The following set of sanctions shall be enforced for any violation by a Bidder of its commitments or undertakings under the Integrity Pact:

(i) Denial or loss of contracts;
(ii) Forfeiture of the EMD/Bid security and performance bond/PBG;
(iii) Liability for damages to the principal and the competing Bidders; and
(iv) Debarment of the violator by NHB for an appropriate period of time.

The Bidders are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behavior compliance program for the implementation of the code of conduct throughout the company).

Annexures

Annexure – I (Bidder's Information)

Please provide following information about the Company (Attach separate sheet if required): -

S. No.	Information	Particulars / Response		
1.	Name of the firm			
2.	Date of Incorporation			
3.	Type of firm [Govt/PSU/Pub. Ltd / Pvt. Ltd/partnership/proprietary]			
4.	Registration No. and date of registration. **Registration Certificate to be enclosed**			
5.	Address of Registered Office with contact numbers [phone /fax]			
6.	PAN No			
7.	**Contact Details of Bidder authorized to make commitments to NHB**			
8.	Name			
9.	Designation			
10.	FAX No			
11.	Mail ID			
12.	Company Head Office and Addresses Contact Person(s) Phone Fax E-mail Website			
13.	Any pending or past litigation (within three years)? If yes please give details Also mention the details of claims and complaints received in the last three years (About the Company / Services provided by the company).	Yes/No/Comments (if option is 'Yes') (If option is 'Yes' Bidder may Not be considered)		
14.	Please mention turnover and Net Profit/Loss for last three years and include the copies of Balance Sheet in support of it.	Year	Turnover	Net Profit/Loss(-)

Audited/CA certificate of Balance sheet and Profit & Loss accounts for last 3 years to be submitted.

Authorized Signatories
(Name & Designation, seal of the company)

Date:

Annexure – II (Bidder Experience Details)

1.	Bidder's experience in Cyber Security field _____ (in years)	
	a) Experience in India	
	b) Global experience	
2.	Details of service contracts on _____ executed with Public Sector **B**anks/All India FIs/in India.	
3.	No. of qualified personnel employed	
4.	Number of operating offices in India	
5.	Details of Operating Offices in India	

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure – III (Compliance Statement Declaration)

We hereby undertake and agree to abide by all the terms and conditions stipulated by NHB in this RFP including all addendum, corrigendum etc. (Any deviation may result in disqualification of Bids).

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure – IV (List of Deviations)

We certify that the services offered by us for tender confirms to the requirement stipulated as per this RFP with the following deviations

Bidders are requested to provide details of all deviations, comments and observations or suggestions in the following format with seal and signature. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.

NHB may at its sole discretion accept or reject all or any of the deviations, however it may be noted that the acceptance or rejection of any deviation by NHB will not entitle the Bidder to submit a revised Bid.

List of deviations

1) _____
2) _____
3) _____

(If left blank it will be construed that there is no deviation from the specifications given above)
(The decision of NHB is final towards evaluation of the Bid documents)

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure –V (Minimum Eligibility Criteria)

S No	Criteria
1.	The Bidder must be an ISO 27001 certified organization and should be a Private Limited of Limited Company
2.	During last five years (i.e. between 01.4.2014 to 31.03.2019) the Bidder should have carried out the work of implementation of cyber security framework in at least one SCB/All India FI, having investment size of more than Rs. 1000 Crore as on March 31, 2019).
3.	The Bidder must be empanelled with CERT-In as Information Security Audit Organization
4.	The bidder Company should have at-least 25 qualified Information Security / Cyber Security professionals (DISA/CISA/CISM/CDAC/ CEH) in their payroll.
5.	The Bidder should have its own office in Delhi NCR and Mumbai Metropolitan Region (MMR).
6.	The Bidder firms should not have been black listed/ debarred by any Government Financial Institutions /Banks/ RBI/ ICAI/ IBA / Government / Semi Government Departments/ PSUs / in India during last 5 years and Blacklisting should not be in force.
7.	The Bidder should not be owned or controlled by any Director or Employee of National Housing Bank, both present and those who have retired in the last two Years, or by any of their Relatives. Further, the Bidder shall not engage any of the foregoing persons as partners, employees or contractors for any work whether connected with the "Assignment/ Job/ Engagement" nor shall they benefit directly or indirectly from the "Assignment/ Job/ Engagement" in any manner.
8.	Average annual professional income from information / cyber security activities of the firm during last three years i.e. 2016-17, 2017-18 & 2018-19 should be minimum Rs. 10 Crore.

Annexure – VI (Technical Bid Covering Letter)

Date:

To
The _____
National Housing Bank,
All Audits Department
Head Office
Core 5-A, 3rd Floor, India Habitat Centre, Lodhi Road,
New Delhi – 110003

Dear Sir,

Technical Bid – Preparation of Cyber Security Framework

We, the undersigned, offer to provide services for the above-mentioned assignment, in accordance with your RFP document [Insert RFP Number] dated [Insert Date]. We are hereby submitting our Proposal, which includes Minimum Eligibility Criteria, this Technical Proposal and a commercial Proposal. The minimum eligibility criteria and technical proposal are put in one envelope and the commercial proposal in separate envelope.

We understand you are not bound to accept any proposal you receive.

Dated at _____ / _____ day of _____ 2019.

Yours faithfully,
For

Signature
Name:

Address:
(Authorised Signatory)

Annexure –VII (Technical Bid Format)

Bidder response to the Technical Bid of this RFP document must be provided as detailed in chapter 7. Any extra information may be provided as separate section at the end of Technical Bid document. Technical Bid should be submitted with covering letter.

1. **Details as detailed as below mentioned under Table 1:____**
2. **List of deviations** (as per Annexure -IV)
3. **Technical Bid Covering Letter** (as per Annexure –VI)
4. Others as described above.

Note: Bidder must submit softcopy of complete technical Bid inside the sealed envelope meant for 'Technical Proposal".

Table 1 :

S No	Details	Marks
	Part I	
1.	Existence of the firm in the field of providing Information Security / Cyber Security Services (Max Marks 15) More than 15 More than 10 but ≤ 15 Years More than 05 but ≤ 10 Years	 15 10 05
2.	The number of professional staff (excluding typists, stenographers, computer operators, secretary/ies and subordinate staff etc.) in the area of Information Security / Cyber Security (Bidder will provide a list of staff signed by authorized signatory on their letter head which will include Qualification, designation, No of year of Experience etc.) (Max Marks: 15) More than 75	 15

	More than 40 but ≤ 75 More than 25 but ≤ 40	10 05
3.	No. of SCBs/All India FIs/ PSBs, where the vendor has carried out implementation of Cyber Security Framework More than 5 More than 3 but ≤ 5 More than 1 but ≤ 3	 15 10 05
4.	No of satisfactory service certificate issued by client pertaining to implementation of Cyber Security Framework More than 5 More than 3 but ≤ 5 More than 1 but ≤ 3	 15 10 05
5.	Average annual professional income of the firm during last three years i.e. 2016-17, 2017-18 and 2018-19 (Max Marks: 15) More than 20 Crore More than 15 but ≤ 20 Crore More than 10 but ≤ 15 Crore	 15 10 05
	Part II	
6.	Presentation on proposed roadmap for implementation of Cyber Security Framework and setting-up of C-SOC	25

Annexure –VIII (Commercial Bid Covering Letter)

The _____
National Housing Bank,
All Audits Department
Head Office,
Core 5-A, 3rd Floor, India Habitat Centre, Lodhi Road,
New Delhi – 110003

Dear Sir,

Commercial Bid for preparation of Cyber Security Framework

We, the undersigned, offer to provide services for the above-mentioned assignment, in accordance with your Request for Proposal [_____Insert RFP Number] dated [_____], and our Proposal (Technical and Commercial Proposals). The Total fee is exclusive of all taxes, duties, charges and levies (as applicable and payable under the laws) and out of pocket expenses that we might incur and there will be no additional charges.

Our commercial proposal shall be binding upon us, subject to the modifications resulting from contract discussions, up to expiration of the validity period of the Proposal i.e. _____up to _____[date].

Yours faithfully,
For …….

Signature

Name
Address

(Authorised Signatory)
Date:

Annexure –IX (Commercial Bid Format)

The structure of the Bidder's commercial response to this RFP must be as per following order. The Commercial Bid Response must be submitted with Commercial Bid covering letter, format of which is given at the end this section.

S. No.	Services	Price in (INR)
1.	Consultancy Charges towards preparation of Cyber Security Framework including Charges for facilitation of setting up of CSOC	

* **Including mandatory manpower sought under Scope of work.**

Bidders are requested to note the following:

- All the details must be provided as per format. Incomplete formats will result in rejection of the proposal.
- Masked commercial Bids must be given with technical Bid. All the pages of commercial Bids must be sealed and signed by authorized signatory.
- All the quoted costs will be exclusive of GST but inclusive of all other taxes, duties, charges, cess (if any).
- Bidder must submit softcopy of complete commercial Bid inside the sealed envelope meant for 'Commercial Proposal'.
- All the rates must be quoted in INR.
- 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 commercial Bid. Failure to do so will make the Bid liable to be rejected.
- The commercials quoted in the commercial Bid are valid for six months from the date of opening of commercial Bids. After selection the price quoted will be valid during the currency of project.

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure – X (ECS MANDATE)

[To be submitted along with Technical Bid]

ECS MANDATE

FORM FOR PROVIDING DETAILS OF BANK ACCOUNT FOR CREDIT OF PAYMENT FROM NATIONAL HOUSING BANK

(Please fill in the information in CAPITAL LETTERS)

1. Name of the Bidder _____

2. Address of the Bidder _____

City: _____ Pin Code: _____

E-mail id: _____

Phone /Mobile No. _____

Permanent Account Number (PAN) _____

Service Tax Registration No. _____

TIN No. _____

3. Particulars of Bank Account

A. Name of Account same as in the Bank: _____

B. Name of the Bank: _____

C. Name of the Branch: _____

D. Address of the Branch with Tel No. _____

_____

E. Account No. (appearing in Cheque book): _____

F. Account Type (SB, Current, etc.): _____

G. MICR No. _____

H. IFSC Code of the bank branch: _____

I/We hereby authorize National Housing Bank to credit payment(s) to my/our above bank account by ECS. # (#ECS will accepted on centers where the facility is available).

I/We hereby declare that the particular given above are correct and complete. If the transaction is delayed or not effected at all by ECS for reasons of incomplete or incorrect information, I/we would not hold National Housing Bank responsible. I also undertake to advise any change in the particulars of my account to facilitate updation of records for purpose of credit of amount through RTGS/NEFT.

I also agree that without prejudice to the generality of the foregoing, in the event National Housing Bank is not able to carry out the ECS instructions given by me, National Housing Bank may make such arrangements for payment as deemed appropriate by it, for effecting the transaction.

Place:
Date: Authorized Signatory/ies

Certified that the particulars furnished above are correct as per our records.

Bank's Stamp:

Date:
Signature of the Authorized Official of the Bank

Annexure XI (Letter of Competence Format)

[To be submitted along with Technical Bid]

[To be executed on a non- judicial stamp paper]

Letter of Competence for Quoting against NHB's RFP No. /……..

This is to certify that we _____ [Insert name of Bidder], Address _____ are fully competent to undertake and successfully deliver the scope of services mentioned in the above RFP. This proposal is being made after fully understanding the objectives of the project and requirements like experience etc.

We certify that the quality and number of resources to be deployed by us for the purpose will be adequate to meet the requirement and provide the services professionally and competently.

We also certify that all the information given by in response to this RFP is true and correct.

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure XII (Curriculum Vitae (CV) of Key Personnel)

Marks will be awarded where complete details are provided. It is mandatory that Bidder to provide details of project handled, brief of the assignment, period for each of the resource proposed relevant to scope of the tender. Each resource deployed shall provide self-certificate indicating relevant experience of tender scope.

Format

1) Proposed Position [only one candidate shall be nominated for each position Expert]:
2) Resource Name:
3) Nationality:
4) Date of Birth
5) Educational Qualifications:
   [Indicate college/university and other specialized education of staff member, giving names of institutions, degrees obtained, and dates of obtainment]:
6) Certifications **and Trainings attended**:
7) No. of years‟ of experience
8) Total No. of years with the firm
9) **Areas of expertise and no. of years of experience in this area (as required for the Profile - mandatory)**:

Sno	Project Name	Year & Period spent on project	Brief of the Project	Project Relevance to scope of work of this RFP (section details)	Project Customer Name, Contact Details & Address

10) **Languages** [For each language indicate proficiency: good, fair, or poor in speaking, reading, and writing]**:**

11) **Membership of Professional Associations:**

12) **Employment Record** [Starting with present position and last 2 firms, list in reverse order, giving for each employment (see format here below): dates of employment, name of employing organization, positions held.]:

From (Year): To (Year):

Purchaser:

13) Positions held:

Detailed Tasks Assigned	**Relevant Work Undertaken that Best Illustrates the experience as required for the Role (provide maximum of 6 citations of 10 lines each)** (Among the assignments in which the staff has been involved, indicate the following information for those assignments that best illustrate staff capability to handle the tasks listed under point 14 and as required for the role as listed in „List of the key professional positions whose CV and experience would be evaluated") Name of assignment or project: Year: Location: Purchaser: Main project features: Positions held: Value of Project (approximate value or range value):

14) Certification:

I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes myself, my qualifications, and my experience. I understand that any wilful misstatement described herein may lead to my disqualification or dismissal, from the assignment if engaged.

Date:

(Signature of staff member or authorized representative of the staff)

Full name of Authorized Representative:

Annexure XIII (Escalation Matrix)

We declare that we will adhere to following Escalation matrix during our service contract period with NHB:

Levels	Name of the Concerned person , Designation and Contact Details
Level 1 Escalation	
Level 2 Escalation	
Level 3 Escalation	

Annexure XIV Pre Contract Integrity Pact

(To be executed on a non- judicial stamp paper)

This pre-bid/pre-contract Agreement (hereinafter called "**this Integrity Pact**") between, the National Housing Bank, a bank established under the provisions of the National Housing Bank Act, 1987 having its Head Office at Core 5A, India Habitat Centre, Lodhi Road, New Delhi-110003 represented through Shri/Ms _____ , (Designation) (hereinafter called "NHB", which expression shall mean and include, unless the context otherwise requires, its successors in office and assigns) of the First Part

AND

M/s _____ represented by Shri_____, Chief Executive Officer (hereinafter called the "Bidder" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

(The party of the First Part and the party of the Second Part are hereinafter collectively referred to as the ***"Parties"*** *and individually as the* ***"Party"****)*

WHEREAS NHB proposes to procure _____ (name of the items/services) as mentioned in the RFP No._____ ("RFP") and the Bidder is willing to offer/has offered _____ (name of the items/services) as desired by NHB in terms of the RFP;

WHEREAS the Bidder is a private company/public company/Government undertaking/ partnership/registered export agency, constituted in accordance with the relevant law in the matter and NHB is a statutory body established under the Act of Parliament;

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

(i) enabling NHB to obtain the desired said stores/equipment/services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement and
(ii) enabling Bidders to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and NHB will commit to prevent corruption, in any form, by its officials by following transparent procedures.

AND WHEREAS the Parties hereto hereby agree to enter into this Integrity Pact on the terms and conditions mentioned hereinafter.

NOW IT IS THEREFORE AGREED BY AND BETWEEN THE PARTIES HERETO AS

FOLLOWS:

1. Commitments of NHB

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

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

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

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

3. Commitments of Bidders

3.1 Compliance of the Instructions of GOI/Guidelines of CVC/Others: The Bidder undertakes that in case of its selection as the successful Bidder, it shall perform its duties under the Contract in strict compliance of the relevant and extant instructions of Government of India, GFR issued by Ministry of Finance, Guidelines of CVC and provisions of the Procurement Manual/relevant instructions of NHB, as applicable to the subject matter.

3.2 The Bidder represents that it has the expertise to undertake the assignment/contract and also has the capability to deliver efficient and effective advice/services to NHB under the contract in terms of the RFP.

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

(a) The Bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of NHB,

connected directly or indirectly with the Bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the Bidding, evaluation, contracting and implementation of the contract.

(b) The Bidder has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees , brokerage or inducement to any official of NHB or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Government.

(c) The Bidder shall disclose the name and address of its agents and representatives including its foreign principals or associates.

(d) The Bidder shall disclose the payments to be made by it to agents/brokers or any other intermediary, in connection with this Bid/contract.

(e) The Bidder has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to NHB or any of its functionaries, whether officially or unofficially to the award of the contract to the Bidder, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect or any such intercession, facilitation or recommendation.

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

(g) The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, Bid evaluation, contracting and implementation of the contract.

(h) The Bidder will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

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

(j) The Bidder commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

(k) The Bidder shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

(l) If the Bidder or any employee of the Bidder or any person acting on behalf of

the Bidder, either directly or indirectly is a relative of any of the officers of NHB or alternatively, if any relative of an officer of NHB has financial interest/stake in the Bidders firm, the same shall be disclosed by the Bidder at the time of filing of tender.

The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

(m) The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of NHB.

(n) The Bidders shall disclose any transgressions with any other company that may impinge on the anti-corruption principle.

(o) The Bidder has not entered into any undisclosed agreement or understanding with other Bidders with respect of prices, specifications, certifications, subsidiary contracts, etc.

3.4 The Bidder undertakes and affirms that it shall take all measures necessary to prevent any possible conflict of interest and in particular commit itself to the following:

(a) The Bidder shall avoid any conflict of interest while discharging contractual obligations and bring, beforehand, any possible instance of conflict of interest to the knowledge of NHB, while rendering any advice or service.

(b) The Bidder shall act/perform, at all times, in the interest of NHB and render any advice/service with highest standard of professional integrity.

(c) The Bidder undertakes that in case of its selection as the successful Bidder, it shall provide professional, objective, and impartial advice and at all times and shall hold NHB's interests paramount, without any consideration for future work, and that in providing advice it shall avoid conflicts with other assignments and its own interests.

(d) The Bidder declares/affirms that it has not been hired by NHB for any assignment that would be in conflict with its prior or current obligations to other employers/buyers, or that may place it in a position of being unable to carry out the assignment/contract in the best interest of NHB. Without limitation on the generality of the foregoing, the Bidder further declares/affirms as set forth below:

(i) **Conflict between consulting activities and procurement of goods, works or non-consulting services (i.e. services other than consulting services)** - The Bidder has not been engaged by NHB to provide goods, works, or non-consulting services for a project, or any affiliate that directly or indirectly controls, is controlled by, or is under common control with the Bidder. The Bidder is fully aware that it shall be disqualified from providing consulting services resulting from or directly related to those goods, works, or non-consulting services. Further, the Bidder is also aware of the fact that in case it has been hired to provide consulting services for the preparation or implementation of a project, or any affiliate that directly or indirectly

controls, is controlled by, or is under common control with the firm, shall be disqualified from subsequently providing goods, works, or services (other than consulting services) resulting from or directly related to the consulting services for such preparation or implementation.

This provision does not apply to the various firms (consultants, contractors, or suppliers) which together are performing the Bidder's obligations under a turnkey or design and build contract.

(ii) **Conflict among consulting assignments** – The Bidder understands that neither Bidder (including their personnel and sub-consultants), nor any affiliate that directly or indirectly controls, is controlled by, or is under common control with the firm, shall be hired for the assignment that, by its nature, may be in conflict with another assignment of the Bidder. *As an example, Bidders assisting NHB in the privatization of public assets shall neither purchase, nor advise purchasers of, such assets. Similarly, Bidders hired to prepare Terms of Reference (TOR) for an assignment shall not be hired for the assignment in question.*

(iii) **Relationship with NHB's staff** – The Bidder is aware that the contract may not be awarded to the Bidder in case it is observed that it, including its experts and other personnel, and sub-consultants, has/have a close business or family relationship with a professional staff of NHB (or of the project implementing agency) who are directly or indirectly involved in any part of: (i) the preparation of the TOR for the assignment, (ii) the selection process for the contract; or (iii) the supervision of such contract, unless the conflict stemming from this relationship has been resolved in a manner acceptable to NHB throughout the selection process and the execution of the contract.

(iv) **A Bidder shall submit only one proposal either individually or as a joint venture partner in another proposal:** If the Bidder, including a joint venture partner, submits or participates in more than one proposal, all such proposals shall be disqualified. This does not, however, preclude a consulting firm to participate as a sub-consultant, or an individual to participate as a team member, in more than one proposal when circumstances justify and if permitted by the RFP.

4. Previous Transgression

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

4.2 The Bidder agrees that if it makes incorrect statement on this subject, Bidder can be

disqualified from the tender process or the contract, if already awarded can be terminated for such reason.

5. Accountability

5.1 The Bidder undertakes that in case of its selection as the successful Bidder and assignment of the contract to the Bidder, it shall be accountable for the advice/supply made/to be made and/or for any service rendered/to be rendered by it to NHB, keeping in view norms of ethical business, professionalism and the fact that such advice / services to be rendered by it for a consideration.

5.2 The Bidder shall be accountable in case of improper discharge of contractual obligations and/or any deviant conduct by the Bidder.

6. Personal Liability

The Bidder understands that in case of its selection as the successful Bidder, the Bidder is expected to carry out its assignment with due diligence and in accordance with prevailing standards of the profession. The Bidder shall be liable to NHB for any violation of this Integrity Pact as per the applicable law, besides being liable to NHB as may be provided under the service level agreement/contract to be executed.

7. Transparency and Competitiveness

The Bidder undertakes that in case of its selection as the successful Bidder, it shall keep in view transparency, competitiveness, economy, efficiency and equal opportunity to all prospective tenderers/Bidders, while rendering any advice/service to NHB, in regard with matters related to selection of technology and determination of design and specifications of the subject matter, Bid eligibility criteria and Bid evaluation criteria, mode of tendering, tender notification, etc.

8. Co-operation in the Processes:

The Bidder shall cooperate fully with any legitimately provided/constituted investigative body, conducting inquiry into processing or execution of the consultancy contract/any other matter related with discharge of contractual obligations by the Bidder.

9. Sanctions for Violations

9.1 Any breach of the aforesaid provisions by the Bidder or any one employed by it or acting on its behalf (whether with or without the knowledge of the Bidder) shall entitle NHB to take all or any one of the following actions, whenever required:

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the Bidder. However the proceedings with the other Bidder(S) would continue.

(ii) The Earnest Money Deposit (in per-contract stage) and / or Security Deposit /Performance Bond/PBG (after the contract is signed) shall stand forfeited either fully or partially, as decided by NHB and NHB shall not be required to assign any reason therefor.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the Bidder.

(iv) To recover all sums already paid by NHB, and in case of an Indian Bidder with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a Bidder from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the Bidder from NHB in connection with any other contract, such outstanding payment could also be utilized and appropriated by NHB to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the Bidder, in order to recover the payments already made by NHB, along with interest.

(vi) To cancel all or any other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to NHB resulting from such cancellation /rescission and NHB shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

(vii) To debar the Bidder from participating in future Bidding process of NHB for a minimum period of five year which may be further extended at the discretion of NHB.

(viii) To recover all sums paid in violation of this Integrity Pact by Bidder(S) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by NHB with the Bidder, the same shall not be opened.

(x) Forfeiture of Performance Bond/PBG in case of a decision by NHB to forfeit the same without assigning any reason for imposing sanction for violation of this Integrity Pact.

9.2 NHB will be entitled to take all or any the actions mentioned at para 10.1(i) to (x) of this Integrity Pact also on the Commission by the Bidder or any one employed by it or acting on its behalf (whether with or without the knowledge of the Bidder), of an offence as defined in Chapter IX of the Indian Penal Code, 1860 or Prevention or Corruption Act, 1988 or any other statute enacted for prevention of corruption.

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

10. Fall Clause:

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

11. Disqualification & Forfeiture of EMD/PBG etc

The Bidder(s) agree(s) that:

(a) Prior to award of contract or during execution of the contract, if the Bidder (s) has/have committed any transgression/breach of this Integrity Pact, NHB is entitled to disqualify the Bidder(s) from the tendering process/terminate the contract.

(b) If NHB disqualifies the Bidders(s) from the tendering process prior to award of contract under clause (a) above, NHB is entitled to demand and recover the damages equivalent to the EMD and in such event, the EMD shall be forfeited.

(c) After selection of the successful Bidder and/or during execution of the contract, any breach/violation by the successful Bidder of this Integrity Pact under clause (a) above shall entail forfeiture of performance bond/Performance Bank Guarantee (PBG).

(d) It is agreed that the decision of NHB regarding forfeiture of EMD/performance bonds/ PBG shall be final and binding.

12. Independent External Monitors:

12.1 NHB has appointed Shri Kishore Kumar Sansi, Ex-MD of Vijaya Bank (email id kishoresansi1@gmail.com) and Shri Rakesh Rewari, Ex-DMD, SIDBI (email id : r_rewari@yahoo.com) as independent external monitors (hereinafter referred to as "the Monitors") for this Integrity Pact in consultation with the Central Vigilance Commission.

12.2 The task of the Monitors shall be to review independently and objectively whether and to what extent the Parties comply with the obligations under this Integrity Pact.

12.3 The Monitors shall not be subject to instructions by the representatives of the Parties

and perform their functions neutrally and independently.

12.4 Both the Parties accept that the Monitors have the right to access all the documents relating to the project procurement including minutes of meeting.

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

12.6 The Bidder accepts that the Monitor has the right to access without restriction to all project documentation of NHB including that provided by the Bidder. The Bidder will also grant the Monitor upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to sub-contractors. The Monitor shall be under contractual obligation to treat the information and documents (s) of the Bidder/sub-contractor with confidentiality.

12.7 NHB will provide to the Monitor sufficient information about all meetings among the Parties related to the project provided such meeting could have an impact on the contractual relations between the Parties. The Parties will offer to the Monitor the option to participate in such meeting.

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

13. Facilitation of Investigation:

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

14. Law and Place of Jurisdiction:

This Integrity Pact is subject to Indian Law. Any dispute arising out of this shall be subject the jurisdictions of the Courts at New Delhi.

15. Other Legal Action:

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provision of the extant law in force relating to any civil or criminal proceedings. However, the Parties shall not approach the Courts of Law while representing the matters to the Monitor/s and shall await the decision of the Monitor/s in the matter.

16. Validity:

16.1 The validity of this Integrity Pact shall be from date of its signing and extend up to

5 years or the complete execution of the contract to the satisfaction of both NHB and the Bidder, including warranty period, whichever is later. In case Bidder is unsuccessful, this Integrity Pact shall expire after six month from the date of the signing of this Integrity Pact.

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

The Parties hereto sign this Integrity Pact on the day, month and year and at the place mentioned herein below.

For National Housing Bank	**For Bidder**
(Authorised Signatory)	**(Authorised Signatory)**
Place: **Date:**	**Place:** **Date:**
Witness **1.**_____ _____ **(Name & Address)** **2.**_____ _____ **(Name & Address)**	**Witness** **1.**_____ _____ **(Name & Address)** **2.**_____ _____ **(Name & Address)**

Annexure XV (Service Level Agreement)
(To be executed on a non- judicial stamp paper)
Service Level Agreement

THIS SERVICE LEVEL AGREEMENT (hereinafter referred to "the **Agreement**") is made on this _____ day of the month of _____, 201_, by and between,

National Housing Bank, a bank constituted under the National Housing Bank Act, 1987, having its Head Office at Core 5A, 3rd -5th floors, India Habitat Centre, Lodhi Road, New Delhi-110003 (hereinafter called "**NHB**",) which expression shall include wherever the context so permits, its successors and assigns ; AND

_____, a company registered under the Companies Act, 1956, having its registered office at _____ (hereinafter called the **"**Consultants**")**, which expression shall include wherever the context so permits, its successors and permitted assigns.

(Hereinafter NHB and the Consultants are collectively referred to as "the Parties" and individually as "the Party")

WHEREAS

(A) NHB intends to hire the Consultants for _____, as detailed in the Request for Proposal no. _____ on _____ (date) (including Corrigendum/Clarification, if any, issued) (hereinafter collectively referred to the "**RFP** (attached hereto as **Appendix-** I).

(B) The Consultant has been selected through open tendering process by way of floating the RFP by NHB followed by evaluation of Technical & Commercial Bids of the Bidders and accordingly the letter of award no. _____ dated _____ ("LoA") (attached hereto as **Appendix-** II) has been issued by NHB to the Consultant;

(C) The Consultant has accepted and agreed to provide the Services in accordance with terms and conditions of RFP and the LoA.

(D) In terms of the RFP, NHB and the Consultant have agreed to enter into this definitive Service Level Agreement in the manner hereinafter appearing:

NOW THEREFORE the Parties hereby agree as follows:

1. GENERAL PROVISIONS

1.1 Definitions

Unless the context otherwise requires, the following terms whenever used in this Agreement have the following meanings:

(a) "Applicable Law" means the laws and any other instruments having the force of law in India, as they may be issued and in force from time to time;

(b) "Contract" means and shall construe this Agreement;

1. "Deliverables" means and includes the major deliverables as specified in Clause 5 of the RFP.

(d) "Effective Date" means the date on which this Agreement comes into force and effect pursuant to Clause 2.1 hereof;

(e) "Personnel" means persons hired/to be hired by the Consultant as employees and assigned to the performance of the Services or any part thereof.

(f) "Project" means collectively the Services and the Deliverables to be provided as detailed in the RFP.

(g) "Services" or "Scope of Work" means and includes the scope of work to be performed by the Consultant as described/set out in Clause 5 of the RFP.

(h) "Third Party" means any person or entity other than NHB and the Consultant.

1.2 Principles of Interpretation

In this Agreement , unless the context otherwise requires:

a) All capitalized terms unless specifically defined in this Agreement shall have the meaning given to them in the RFP;

b) Words and abbreviations, which have well known technical or trade/commercial meanings are used in this Agreement in accordance with such meanings;

c) The RFP, the LoA and the NDA along with the Appendices/ Attachments hereto, shall form part and parcel of this Agreement and shall be read together for all purpose and effect.

d) In case of any inconsistency or repugnancy between the provisions contained RFP, LoA and this Agreement, unless the context otherwise requires, the opinion of NHB shall prevail to the extent of such inconsistency or repugnancy and the same shall be binding on the Consultant.

1.3 Purpose

1.3.1 It is hereby agreed that the Consultant shall provide the Services to NHB as set out in the RFP till the completion of the Project. The objective of the Project is to make _____.

1.3.2 Performance of the Scope of Work

The Consultant shall perform all the services as set out in the Scope of Work and complete the Deliverables within the prescribed time lines in terms of the RFP and the entire assignment shall be completed within the Term of this Contract.

1.3.3 Term/Period of Contract

The entire assignment as detailed in the Scope of Work under this Contract shall be completed within a period of _____ (**"Term")** starting from _____ by the Consultant unless the period is extended in accordance with this Agreement.

1.3.4 Contract Price

The entire assignment to be performed under this Contract is fixed price contract and the Consultant shall be paid the total price consideration of Rs. _____ (Rupees _____) (**"Contract Price**") for the satisfactory performance/execution of the entire assignment under the Project. The Contract Price shall be paid by NHB as per the payment terms agreed at Clause 4.2 of this Agreement.

1.4 Relation between the Parties

Nothing contained herein shall be construed as establishing a relationship of master and servant or of principal and agent as between NHB and the Consultant. The Consultant, subject to this Agreement, has complete charge of personnel to be engaged by the Consultant for performing the Services and shall be fully responsible for the works to be performed by them or on their behalf hereunder and also for the quality of the work done by their personnel.

1.5 Language

This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.6 Headings

The headings shall not limit, alter or affect the meaning of this Contract.

1.7 Notices

1.7.1 Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram or facsimile to such Party at the following address:

For NHB:
Attention:_____
Fax:_____

For the Consultant:
Attention:_____
Fax:_____

1.7.2 Notice will be deemed to be effective as follows

(a) In the case of personal delivery or registered mail, on delivery;

(b) In case of telegrams, ninety six (96) hours following confirmed transmission; and

(c) In the case of facsimiles, seventy two (72) hours following confirmed transmission.

1.7.3 A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to this Clause.

1.8 Location

The Services shall be performed at Delhi or at such location required/ approved by NHB.

1.9 Authority of Consultant

The Consultant hereby authorize _____ to act on their behalf in exercising the entire Consultant's rights and obligations towards NHB under this Contract, including without limitation for signing letters/communications, execution of agreements, for receiving instructions and payments from NHB.

1.10 Taxes and Duties

The Consultants and their personnel shall pay the taxes (excluding GST), duties, fees, levies and other impositions levied under the existing, amended or enacted laws during the tenure of this Agreement and NHB shall perform such duties in regard to the deduction of such taxes as may be lawfully imposed from the payments to be made to the Consultant.

2.0 COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

2.1 Effectiveness of Contract

This Agreement deemed to have taken effect from the date of acceptance of the Letter of Award (LoA) by the Consultant i.e. w.e.f. …….

2.2 Commencement of Services

The Consultant shall begin carrying out the Services immediately viz. from the date of acceptance of LoA, or on such date as the Parties may agree in writing.

2.3 Expiration of Contract

Unless terminated earlier pursuant to Clause-2.8 hereof, this Contract shall expire on the expiry of the Term as stated on Clause 1.3.3 herein unless the Term is extended in accordance with the Clause 2.6.4.

2.4 Entire Agreement

This Contract contains all covenants, stipulations and provisions agreed by the Parties. No representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

2.5 Modification

Modification of the terms and conditions of this Contract, including any modification of the scope of the Services/Scope of Work, may only be made by written agreement between the Parties and shall not be effective until the consent of the Parties has been obtained, pursuant to Clause-5.2 hereof, however, each Party shall give due consideration to any proposals for modification made by the other Party.

2.6 Force Majeure

2.6.1 Definition

In the event of either Party being rendered unable by Force Majeure to perform any obligation required to be performed by them under the Contract, the relative obligation of the Party affected by such Force Majeure shall be suspended for the period during which such cause lasts.

The term "Force Majeure" as employed herein shall mean acts of God, War, Civil Riots, Fire, Flood and Acts and Regulations of respective government of the two Parties directly affecting the performance of the Contract.

Upon the occurrence of such cause and upon its termination, the Party alleging that it has been rendered unable as aforesaid thereby, shall notify the other Party in writing, the beginning of the cause amounting to Force Majeure as also the ending of the said clause by giving notice to the other Party within 72 hours of the ending of the cause respectively. If the deliveries are suspended by Force Majeure conditions lasting for more than 2 (two) months, NHB shall have the option of canceling this Contract in whole or part at its discretion without any liability on its part.

Time for performance of the relative obligation suspended by Force Majeure shall then stand extended by the period for which such cause lasts.

2.6.2 No Breach of Contract

The failure of a Party to fulfill any of its obligations hereunder shall not be considered to be a breach of or default under this Contract in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all reasonable precautions, due care and reasonable alternative measures, all with the objective of carrying out the terms and conditions of this Contract.

2.6.3 Measures to be taken

(a) A Party affected by an event of Force Majeure shall take all reasonable measures to

remove such Party's inability to fulfill its obligations hereunder with a minimum of delay.

(b) A Party affected by an event of Force Majeure shall notify the other Party such event as soon as possible, and in any event not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give notice of the restoration of normal conditions as soon as possible.

(c) The Parties shall take all reasonable measures to minimize the consequences of any event of Force Majeure.

2.6.4 **Extension of Time**

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

2.6.5 **Consultation**

Not later than thirty (30) days after the Party, as the result of an event of Force Majeure, has become unable to perform a material portion of the Services, the Parties shall consult with each other with a view to agreeing on appropriate measures to be taken in the circumstances.

2.7 Suspension

NHB may, by written notice of suspension to the Consultant, suspend all payments to the Consultant hereunder if NHB is not satisfied with the performance of the Consultant or if the Consultant fails to perform any of their obligations under this Contract, including the carrying out of services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall request the Consultant to provide remedy for such failure within a period not exceeding thirty (30) days after receipt by the Consultant of such notice of suspension and shall invoke contract performance guarantee.

2.8 Termination

2.8.1 **By NHB**

NHB may by not less than fifteen (15) calendar days written notice of termination to the

Consultant, (except in the event listed in paragraph (g) below, for which there shall be a written notice of not less than sixty (60) days) such notice to be given after the occurrence of any of the events specified in paragraphs (a) to (f) of this Clause-2.8.l, terminate this Contract:

(a) If the Consultant fails to remedy a failure in the performance of their obligations hereunder, as specified in a notice of suspension pursuant to Clause-2.7 here-in-above, within thirty (30) days of receipt of such notice of suspension or within such further period as NHB may have subsequently approved in writing;

(b) If the Consultant becomes insolvent or bankrupt or enters into an agreement with its creditors for relief of debt or take advance of any law for the benefit of debtors or goes into liquidation receivership whether compulsory or voluntary;

(c) If the Consultant fails to comply with any final decision reached/award passed as a result of arbitration proceedings pursuant to Clause-8 hereof;

(d) If the Consultant submits to NHB a statement which has a material effect on the rights, obligations or interests of NHB and which the Consultant knows to be false;

(e) If, as a result of Force Majeure, the Consultant is unable to perform a material portion of the Services for a period of not less than sixty (60) days; or

(f) In the event it comes to the notice of NHB that any of the representations and/or warranties made by the Consultant either in the Bid Documents or in the subsequent correspondences are found to be false and/or the Consultant/its personnel are found to be involved in any fraudulent or criminal act;

(g) If NHB, in its sole discretion and for any reason whatsoever, decides to terminate this Contract..

2.8.2 **Cessation of Rights and Obligations**

Upon termination of this Contract pursuant to Clause- 2.8.1 hereof or upon expiration of this Contract pursuant to Clause-2.3 hereof, all rights and obligations of the Parties hereunder shall cease, except:

(a) Such rights and obligations as may have accrued on the date of termination or expiration,

(b) The obligation of confidentiality set forth in Clause-3.7 hereof,

(c) Any right which a Party may have under the Applicable Law.

2.8.3 **Cessation of Services**

Upon termination of this Contract by notice pursuant to clauses-2.8.1 hereof, the Consultant shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum.

2.8.4 **Payment in case of termination of contract**

Subject to the terms of the RFP, in case the contract is terminated, payment towards services will be made on pro rata basis, for the services already delivered, after deducting applicable penalty and TDS/other applicable taxes.

3.0 OBLIGATIONS OF THE CONSULTANT

3.1 Standard of Performance

The Consultant shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used with professional engineering and consulting standards recognized by professional bodies, and shall observe sound management, technical and engineering practices, and employ appropriate advanced technology, safe and effective equipment, machinery, materials and methods. The Consultant shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to NHB, and shall at all times support and safeguard NHB's legitimate interests in any dealings with third parties.

3.2 Law Governing contract

The Consultant shall perform the assignment in accordance with the applicable Law and shall take all practicable steps to ensure that the Personnel of the Consultant comply with the Applicable Law.

3.3 Conflict of Interest

The Consultant shall hold NHB's interest paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their corporate interests.

3.4 Consultant Not to Benefit from Commissions/Discounts etc.

The payment of the Consultant by NHB shall constitute the Consultant's only payment in connection with this Contract or the Services, and the Consultant shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Consultant shall use their best efforts to ensure that its Personnel similarly shall not receive any such additional payment.

3.5 Consultant and Affiliates not to be otherwise interested in /benefited from the Project

The Consultant agrees that, during the term of this Contract and after its termination, the Consultant shall not create any work/ opportunity for itself and for any of its affiliates from this Project/ assignment and/or derive any financial benefits directly or otherwise, other than what is agreed to be paid as professional fee as mentioned at Clause 4.2 for this assignment.

3.6 Prohibition of Conflicting Activities

The Consultant and its affiliates shall not engage, either directly or indirectly, in any business or professional activities which would conflict with the activities assigned to them under this Contract. The Consultant and its affiliates hired to provide services for the proposed assignment will be disqualified from services related to the initial assignment for the same Project subsequently.

3.7 Confidentiality

The Consultant and its Personnel shall not, either during the term or after the expiration of this Contract, disclose any proprietary or confidential information relating to the Project, the Services, this Agreement or NHB's business or operations without the prior written consent of NHB.

A separate non-disclosure cum confidentiality agreement ("NDA") will be signed between the Consultant and NHB, if required.

3.8 Insurance to be taken out by the Consultant

The Consultant shall take out and maintain at their own cost, appropriate insurance against all the risks, and for all the coverage, like workers compensation, employment liability insurance for all the staff on the assignment, comprehensive general liability insurance, including contractual liability coverage adequate to cover the indemnity of obligation against all damages, costs, and charges and expenses for injury to any person or damage to any property arising out of, or in connection with, the services which result from

the fault of the Consultant or their staff on the assignment

3.9 Liability of the Consultant

The Consultant shall be liable to NHB for the performance of the Services in accordance with the provisions of this Contract and for any loss suffered by NHB as a result of a default of the Consultant in such performance, subject to the following limitations:

(a) The Consultant shall not be liable for any damage or injury caused by or arising out of any act, neglect, default or omission of any persons other than the Consultant and its Personnel; and
(b) The Consultant shall not be liable for any loss or damage caused by or arising out of circumstances over which the Consultant had no control.

3.10 Indemnification of NHB by the Consultant

The Consultant shall indemnify NHB and shall always keep NHB, its employees, personnel, officers and directors, both during and after the term of this Agreement, fully and effectively indemnified against all losses, damage, injuries, deaths, expenses, actions, proceedings, demands, costs and claims, including legal fees and expenses, suffered by NHB or any Third Party, where such loss, damage, injury is the result of (i) any wrongful action, negligence or breach of contract by the Consultant or its personnel; and/or (ii) any negligence or gross misconduct attributable to the Consultant or its personnel; and/or (iii) any claim made by employees who are deployed by the Consultant against NHB; and/or (iv) any claim arising out of employment, non-payment of remuneration and non-provision of benefits in accordance with the statues/various labour laws by the Consultant to its employees; and/or (v) any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or (vi) any breach of the confidentiality obligations mentioned under clause 3.7 and /or NDA.

3.11 Limitation of Liability

(i) The Consultants aggregate liability, in connection with the obligations undertaken as a part of this Project, whether arising under this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), other than the circumstances mentioned in the sub-clause (ii) below, shall be limited to _____ times of the total contract value.

(ii) The Consultant's liability in case of claims against NHB resulting from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations committed by the Consultant shall be actual and unlimited.

(iii) Under no circumstances, NHB shall be liable to the Consultant for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if he has been advised of the possibility of such damages.

3.12 Consultant's Actions Requiring Owner's Prior Approval

The Consultant shall not enter into a sub contract for the performance of any part of the Services, without the prior approval of NHB in writing. However, the Consultant can hire the services of Personnel to carry out any part of the services. The Consultant shall remain fully liable for the performance of the services by its personnel pursuant to this Contract.

3.13 Reporting Obligations

The Consultant shall submit to NHB the reports and documents within the timelines set forth in the Offer Letter, including any supporting data required by NHB.

3.14 Documents prepared by the Consultants to be the Property of NHB:

All reports and other documents prepared/developed by the Consultant in performing the Services shall become and remain the property of NHB, and the Consultant shall, not later than upon termination or expiration of this Contract, deliver all such documents to NHB, together with a detailed inventory thereof. The Consultant may retain a copy of such documents and shall not use them for purposes unrelated to this Contract without the prior written approval of NHB.

3.15 Consultant's Personnel

The Consultant shall ensure that personnel/employees engaged by him in the project/contract, have appropriate qualifications and competence as stipulated under the RFP and are in all respects acceptable to NHB. The Consultant will do its utmost to ensure that the personnel identified by the Consultant to work under this Agreement completes the Term. If any such personnel resigns from his job and leaves the Consultant, the Consultant will provide NHB with another personnel of equivalent knowledge, skill and experience acceptable to NHB as his substitute.

The Consultant shall strictly comply with all applicable labour laws and such other laws in relation to the services to be provided and the personnel engaged by the Consultant and he shall be solely responsible for all acts of the said personnel so enrolled and there shall and will not be any privity of contract for any purpose and to any intent between NHB and said personnel so engaged by the Consultant.

The Consultant shall be responsible for making appropriate deductions in respect of income tax and any other statutory deductions under applicable laws in respect of its personnel/employees engaged by the Consultant under this Agreement. The Consultant agrees to indemnify NHB in respect of any claims that may be made by statutory authorities against NHB in respect of contributions relating to the personnel/employees engaged by the Consultant for performing the work under this Agreement. NHB is authorized to make such tax deduction at source as may be necessary as per law/rules in force in respect of payments made to the Consultant.

3.16 Non-Compete

The Consultant will neither approach nor make any proposal for work for any employee of NHB directly or indirectly during the validity of this Agreement and for one year from the date of termination of this Agreement.

3.17 Change in Ownership or Constitution:

The Consultant will inform NHB immediately about any change in its ownership or its constitution. The Consultant will ensure that the NHB's interest will be protected with utmost care. If NHB is not satisfied with the change of ownership or constitution of the Consultant and/or with the new owner, NHB shall have the right of termination and in that event, the payment, if any, upon termination may be made as provided in clause 2.8.4.

4.0 OBLIGATIONS OF NHB

4.1 Support:

NHB will provide the support as required necessary by it including giving access to the relevant and limited data maintained in its system to the Consultant for carrying out the assignment under the Contract.

4.2 **Consideration & Payment Terms**

In consideration of the Services performed by the Consultant under this Agreement, NHB shall make to the Consultant such payments and in such manner as specified in the RFP and/or the LoA.

The Consultant shall submit the bills to NHB of firms printed bill forms indicating the work done by him during the period for which payment is sought. NHB shall make payments to the Consultant as per the payment schedule given in the RFP. But if the progress is not satisfactory and according to agreed work program/schedule the payment may be withheld.

4.3 Non-Solicitation:

NHB agrees not to make an offer for employment to any personnel provided/deployed by the Consultant under this Agreement, and, not to accept any application for employment from him/her, while he is under the term of this Agreement, and, for up to twelve (12) months from the date of last assignment of the work under this Agreement with NHB.

5.0 FAIRNESS AND GOOD FAITH

5.1 Good Faith

The Parties undertake to act in all fairness and good faith in respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract

6.0 UNDERTAKINGS:

The Consultant hereby further undertakes:

(i) That the Consultant has gone through all the required/relevant and extant instructions/ circulars of Government of India, Reserve Bank of India and /or any other concerned authority, GFR issued by Ministry of Finance, guidelines of CVC and provisions of the manual/relevant instructions of NHB, as applicable to the scope/area of its work/operation under this Agreement and the advice/services to be rendered by it as the Consultant and it complies/will comply with all such requirements.

(ii) That the Consultant has the necessary expertise to work and execute the Project as per the scope of work set out in detail in the RFP and it has the capability to deliver efficient and effective advice/services to NHB. It shall carry out the assignment under this Agreement with due diligence and with the highest standard of professionalism and business ethics.

(iii) That being the Consultant of NHB for a consideration, it shall be accountable for (a) any improper discharge of the assignment under this Agreement and/or (b) any deviant conduct keeping in view the norms of ethical business and professionalism.

(iv) That NHB shall have every right at its discretion to enforce such accountability in case of any improper discharge of contractual obligations and/or any advice/service

rendered in the views of NHB is found to be grossly faulty/negligent/deficient and/or any deviant conduct by the Consultant and as a consequence of it, NHB can, irrespective of anything stated herein, terminate this Agreement by giving 15 days prior notice, including to withhold/retain the dues payable to the Consultant by NHB under this Agreement and appropriate/adjust the same for the losses, if any, suffered by NHB without requiring NHB to prove the actual loss.

(v) That the Consultant shall not do anything that will be of any conflict of interest to the Consultant while discharging the obligations under this Agreement and it shall bring to the notice/knowledge of NHB beforehand any possible instance of conflict of interest while rendering any advice or service. Further, the Consultant shall not receive any remuneration in connection with the assignment except as provided in this Agreement. The Consultant and/or any of its affiliates shall not engage in consulting or other activities that will be in conflict with the obligations under this Agreement.

(vi) That the Consultant has not been hired for any assignment that would be in conflict with its prior or current obligations to NHB or that may place the Consultant in a position of being unable to carry out the assignment in the best interest of NHB.

(vii) That the Consultant shall act at all times in the interest of NHB and render advice/service with highest professional integrity and shall cooperate fully with any legitimately provided/constituted investigative body, conducting inquiry into processing or execution of the consultancy contract/any other matter related with discharge of the contractual obligations by the Consultant.

7.0 SEVERABILITY:

Each clause of this Agreement is enforceable independently. Should any clause of this Agreement become not enforceable due to any reason, it will not affect the enforceability of the other clauses.

8.0 SETTLEMENT OF DISPUTES

In the event of any dispute or difference arising out of, in relation to, or in connection with this Agreement, or the breach thereof, shall be settled amicably through mutual discussions. If, however, the parties are not able to settle them amicably without undue delay, the same shall be settled by the process of arbitration in accordance with the provisions of the Arbitration & Conciliation Act, 1996 (as amended from time to time). The venue of such arbitration shall be at New Delhi and the proceedings shall be conducted in English. The arbitration tribunal shall consist of Sole i.e. 1(one) Arbitrator

to be appointed jointly by the Parties within thirty (30) days from the date of first recommendation for appointment of arbitrator in written form one Party to the other. If the Parties fail to agree on appointment of such Sole Arbitrator, arbitral tribunal consisting of Sole Arbitrator shall be appointed in accordance with the provisions of the Arbitration and Conciliation Act, 1996. The award of arbitrator made in pursuance thereof shall be final and binding on the Parties. All costs and expenses of such arbitration shall be borne equally by the Parties at the first instance which however subject to the provisions of the said Act.

Notwithstanding, it is agreed that the Consultant shall continue the remaining work for the assignment under this Agreement during the pendency of arbitration proceedings unless otherwise directed in writing by NHB or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator, as the case may be, is obtained.

9.0 JURISDICTION AND APPLICABLE LAW

This agreement including all matters connected with this Agreement, shall be governed by the laws of India (both substantive and procedural) for the time being in force and shall be subjected to exclusive jurisdiction of the Courts at New Delhi.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement signed in their respective names on the day and year first above written at New Delhi.

FOR AND ON BEHALF OF NATIONAL HOUSING BANK

By _____

Authorized Representative

FOR AND ON BEHALF OF [CONSULTANT]

By _____

Authorized Representative

WITNESSES:

1.
(Name and address)

2.
(Name and address)

Annexure XVI (Non-Disclosure Agreement)

CONFIDENTIALITY –CUM- NON DISCLOSURE AGREEMENT
(To be executed on a non- judicial stamp paper)

This Confidentiality –cum-Non Disclosure Agreement is entered into at New Delhi on this ……..day ……..of _____, 201__, by and between;

_____, a ……. incorporated _____, having its Registered Office at …… (hereinafter referred to as "the Consultants"), which expression shall include wherever the context so permits, its successors and permitted assigns;

and

The National Housing Bank, a bank constituted under the National Housing Bank Act,1987 (Central act No. 53 of 1987) having its Head Office at Core-5A,5th Floor, India Habitat Centre, Lodhi Road, New Delhi-110003; (herein after referred to as "NHB"), which expression shall include wherever the context so permits, its successors and permitted assigns:

WHEREAS the Consultant & NHB would be having discussions and negotiations concerning _____ ("Purpose") between them as per the Service Level Agreement dated …… (hereinafter referred to as "SLA"). In the course of such discussions & negotiations, it is anticipated that either party may disclose or deliver to the other party certain of its trade secrets or confidential or proprietary information for the purpose of enabling the other party to evaluate the feasibility of such a business relationship. The parties have entered into this Agreement, in order to assure the confidentiality of such trade secrets and confidential & proprietary information in accordance with the terms of this Agreement. As used in this Agreement, the party disclosing Proprietary Information (as defined below) is referred to as "the **Disclosing Party"** & will include its affiliates and subsidiaries, the party receiving such Proprietary Information is referred to as "the **Recipient/Receiving Party"**, and will include its affiliates & subsidiaries and its personnel.

Now this Agreement witnesseth:-

1. **Proprietary Information:** As used in this Agreement, the term Proprietary information shall mean as all trade secrets or confidential or Proprietary information designated as such in writing by the Disclosing Party, whether by letter or by the use of an appropriate prominently placed Proprietary stamp or legend, prior to or at the time

such trade secret or confidential or Proprietary information is disclosed by the Disclosing Party to the Recipient/Receiving Party. Notwithstanding the foregoing, information which is orally or visually disclosed to the Recipient/Receiving Party by the Disclosing party or is disclosed in writing unaccompanied by a covering letter, proprietary stamp or legend, shall constitute proprietary information if the disclosing party , within 10(ten) days after such disclosure, delivers to the Recipient/Receiving Party a written document or documents describing such Proprietary Information and referencing the place and date of such oral ,visual or written disclosure and the names of the employees or officers of the Recipient/ Receiving party to whom such disclosure was made.

2. **Confidentiality:**

a) Each party shall keep secret and treat in strictest confidence all confidential information it has received about the other party or its customers and will not use the confidential information otherwise than for the purpose of performing its obligations under this Agreement in accordance with its terms and so far this may be required for the proper exercise of the Parties respective rights and obligations under this Agreement.

b) The term confidential information shall mean and include all written or oral information (including information received from third parties that the Disclosing Party is obligated to treat as confidential) that is (i) clearly identified in writing at the time of disclosure as confidential and in case of oral or visual disclosure, or (ii) that a reasonable person at the time of disclosure reasonably would assume, under the circumstances, to be confidential. Confidential Information shall also mean, software programs, technical data, methodologies, know how, processes, designs, customer names, prospective customer's names, customer information and business information of the Disclosing Party.

c) Confidential information does not include information which:

(i) is publicly available at the time of its disclosure; or
(ii) becomes publicly available following disclosure; or
(iii) is already known to or was in the possession of Recipient/Receiving party prior to disclosure under this Agreement; or
(iv) is disclosed to the Recipient/Receiving party from a third party, which party is not bound by any obligation of confidentiality; or
(v) is or has been independently developed by the Recipient/Receiving party without using the confidential information;
(vi) is disclosed with the prior consent of the Disclosing Party.

3. **Non –Disclosure of Proprietary Information:** For the period during the agreement or its renewal, the Recipient/Receiving Party will:

   a) Use such Proprietary Information only for the purpose for which it was disclosed and without written authorization of the Disclosing Party shall not use or exploit such Proprietary Information for its own benefit or the benefit of others.

   b) Protect the Proprietary Information against disclosure to third parties in the same manner and with the reasonable degree of care, with which it protects its own confidential information of similar importance and

   c) Limit disclosure of Proprietary Information received under this Agreement to persons within its organization and to those 3rd party contractors performing tasks that would otherwise customarily or routinely be performed by its employees, who have a need to know such Proprietary Information in the course of performance of their duties and who are bound to protect the confidentiality of such Proprietary Information.

4. **Limit on Obligations:** The obligations of the Recipient/ Receiving Party specified in clause 3 above shall not apply and the Recipient/ Receiving Party shall have no further obligations, with respect to any Proprietary Information to the extent that such Proprietary information :

   a) is generally known to the public at the time of disclosure or becomes generally known without any wrongful act on the part of the Recipient/ Receiving Party;

   b) is in the Recipient's/ Receiving Party's possession at the time of disclosure otherwise than as a result of the Recipient's/ Receiving Party's breach of an obligation of confidentiality owed to the Disclosing Party;

   c) becomes known to the Recipient/ Receiving Party through disclosure by any other source, other than the Disclosing party, having the legal right to disclose such Proprietary Information.

   d) is independently developed by the Recipient/ Receiving Party without reference to or reliance upon the Proprietary Information; or

   e) is required to be disclosed by the Recipient/ Receiving Party to comply with applicable laws or governmental regulation, provided that the Recipient/ Receiving Party provides prior written notice of such disclosure to the Disclosing Party and take reasonable and lawful actions for such disclosure.

5. **Return of Documents:** The Recipient/ Receiving Party shall, upon request of the Disclosing Party , in writing ,return to the Disclosing party all drawings, documents and other tangible manifestations of Proprietary Information received by the Recipient/ Receiving Party pursuant to this Agreement (and all copies and reproductions thereof) within a reasonable period. Each party agrees that in the event, it is not inclined to proceed further with the engagement, business discussions and negotiations or in the event of termination of this Agreement, the Recipient/ Receiving Party will promptly return to the other part or with the consent of the other party, destroy the Proprietary Information of the other party. Provided however the Receiving Party shall retain copies to be in compliance with its statutory, regulatory, internal policy or professional obligations.

6. **Communications :**Written communications requesting transferring Proprietary Information under this Agreement shall be addressed only to the respective designees as follows (or to such designees as the parties hereto may from time to time designate in writing)

_____ **NATIONAL HOUSING BANK**

(Consultants)

7. Term: The obligation pursuant to clause 2 and 3 (Confidentiality & Non-Disclosure of Proprietary Information) will survive for a period of _____ years from the termination of the SLA.

8. The provisions of this Agreement are necessary for the protection of the business goodwill of the parties and are considered by the parties to be reasonable for such purposes. Both the parties agree that any breach of this Agreement will cause substantial and irreparable damages to the other party and, therefore, in the event of such breach by one party, the other party shall be entitled to appropriate remedy, which may be available under law.

9. Notwithstanding anything stated in this Agreement, any report/finding/document delivered/submitted by the Consultants to NHB as a part of the outcome or deliverables under the SLA and which, in the opinion of NHB, requires any further study/analysis by any third party agency/institution depending on the requirement of the case, the same can be shared by NHB with such third party agency/institution for conducting such study/analysis and no prior consent of the Consultants is required for the same. Such report/finding/document delivered/ submitted by the Consultants to NHB shall become exclusive property of NHB and as such NHB shall

not be bound by any restriction from disclosure of such report/ finding/ document or content thereof, being the Receiving Party.

10. This Agreement shall be governed and construed in accordance with the laws of India and shall be subjected to the Jurisdiction of courts at Delhi**.** It is agreed that any dispute or differences arising out of or touching this Agreement if not resolved amicably shall be referred to the arbitration as per clause _____ of the SLA executed between the parties hereto.

11. **Miscellaneous**

a) This Agreement may not be modified, changed or discharged, in whole or in part, except by a further Agreement/amendment in writing signed by both the parties.

b) This Agreement will be binding upon & enure to the benefit of the parties hereto and it includes their respective successors & assigns

c) The Agreement shall be construed & and interpreted in accordance with the laws prevailing in India.

In witness whereof, the parties hereto have agreed, accepted and acknowledged and signed these presents, on the day, month and year mentioned herein above.

FOR _____	**FOR NATIONAL HOUSING BANK**
Authorized Signatory	Authorized Signatory
Name:	Name:
Designation:	Designation:
Place:	Place:
Date:	Date:

WITNESSES:

1.

2.

Annexure XVII (Bank Guarantee Format)

(Format of Bank Guarantee)
(To be executed on a non- judicial stamp paper)

To
National Housing Bank
_____,

In consideration of the National Housing Bank (hereinafter referred to as "NHB", which expression shall, unless repugnant to the context or meaning, thereof include its successors, representatives and assignees), having awarded in favour of M/s. _____ having its registered office at _____ (hereinafter referred to as "the Consultants", which expression shall unless repugnant to the context or meaning thereof include its successors, administrators, representatives and assignees), a contract to provide _____ on terms and conditions set out in the Request for Proposal dated…….._____ ("the RFP") and the Service Level Agreement dated _____ ("the SLA") (hereinafter the RFP and the SLA are together referred to as "the Contract"), and the Consultants having agreed to provide a Performance Bank Guarantee for the faithful performance of the services as per the terms of the "Contract" including the warranty obligations /liabilities under the contract of equivalent value amounting to _____/____% of the value of the Contract if any, to NHB amounting to _____ (in words) in the form of a bank guarantee,

, we, _____ (Name) _____(Address) (hereinafter referred to as "the Bank", which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators, representatives and assignees) at the request of the Consultants do hereby irrevocably guarantee for an amount of Rs. _____ (Rupees._____) and undertake to pay NHB the guaranteed amount merely on demand, without any previous notice from NHB, without any demur or protest and without referring to any other source, any and all monies payable by the Consultants by reason of any breach by the said Consultants of any of the terms and conditions of the said Contract including non-execution of the Contract at any time till _____ (day /month/ year). Any such demand made by NHB on the Bank shall be conclusive and binding, absolute and unequivocal not withstanding any disputes raised/pending before any court, tribunal, arbitration or any other authority by and between the Consultants and NHB. The Bank agrees that the guarantee herein contained shall continue to be enforceable till the sum due to NHB is fully paid and claims satisfied or till NHB discharges this Guarantee.

NHB shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee, from time to time, to extend the time of performance by the

Consultants. The Bank shall not be released from its liabilities under these presents by any exercise of NHB of the liberty with reference to the matter aforesaid.

NHB shall have the fullest liberty, without affecting this guarantee to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Consultants and to exercise the same at any time in any manner, and either to enforce or to forbear to enforce any covenants, contained or implied in the Contract between NHB and the Consultants or any other course or remedy or security available to NHB and the Bank shall not be released of its obligations/ liabilities under these presents by any exercise by NHB of his liberty with reference to the matters aforesaid or any of them or by reasons of any other act or forbearance or other acts of omission or commission on part of NHB or any other indulgence shown by NHB or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the Bank Guarantee. The Bank further undertakes not to revoke this guarantee during its currency without the previous consent of NHB in writing.

The Bank further agrees that the decision of NHB as to the failure on the part of the Consultants to fulfil their obligations as aforesaid and/or as to the amount payable by the Bank to NHB hereunder shall be final, conclusive and binding on the Bank.

The Bank also agrees that NHB shall be entitled at his option to enforce this guarantee against the Bank as a principal debtor, in the first instance notwithstanding any other security or guarantee that it may have in relation to the Consultants liabilities.

This guarantee will not be discharged due to the change in the constitution of the Bank or the Consultants.

Notwithstanding anything contained herein:

(a) our liability under this bank guarantee shall not exceed Rs. _____ (Rupees _____in words);

(b) this bank guarantee shall be valid up to _____; and

(c) We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only and only if you serve upon us a written claim or demand on or before _____.

(Signature)
Designation/Staff Code No.
Bank's seal
Attorney as per power of Attorney No. Dated

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2015-16/418
DBS.CO/CSITE/BC.11/33.01.001/2015-16

Jyeshtha 12, 1938 (saka)
June 2, 2016

To

The Chairman/ Managing Director /Chief Executive Officer
All Scheduled Commercial Banks (excluding Regional Rural Banks)

Madam / Dear Sir,

Cyber Security Framework in Banks

Introduction

Use of Information Technology by banks and their constituents has grown rapidly and is now an integral part of the operational strategies of banks. The Reserve Bank, had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (G.Gopalakrishna Committee) vide Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, wherein it was indicated that the measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

2. Since then, the use of technology by banks has gained further momentum. On the other hand, the number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past, more so in the case of financial sector including banks, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis. In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions, if and when they occur.

Need for a Board approved Cyber-security Policy

3. Banks should **immediately** put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their

बैंकिंग पर्यवेक्षण विभाग, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर- I, कफ परेड, कोलाबा, मुंबई -400005
Department of Banking Supervision, Central Office, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005
टेलीफ़ोन/ Tele: +91 22 22189131-39; फैक्स / Fax +91 22 22180157; ईमेल /email : cgmicdbsco@rbi.org.in

Board. A confirmation in this regard may be communicated to Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, Reserve Bank of India, Central Office, World Trade Centre-I, 4th Floor, Cuffe Parade, Mumbai 400005 at the earliest, and in any case not later than September 30, 2016.

It may be ensured that the strategy deals with the following broad aspects:

Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank

4. In order to address the need for the entire bank to contribute to a cyber-safe environment, the Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

5. The size, systems, technological complexity, digital products, stakeholders and threat perception vary from bank to bank and hence it is important to identify the inherent risks and the controls in place to adopt appropriate cyber-security framework. While identifying and assessing the inherent risks, banks are required to reckon the technologies adopted, alignment with business and regulatory requirements, connections established, delivery channels, online / mobile products, technology services, organisational culture and internal & external threats. Depending on the level of inherent risks, the banks are required to identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation. Riskiness of the business component also may be factored into while assessing the inherent risks. While evaluating the controls, Board oversight, policies, processes, cyber risk management architecture including experienced and qualified resources, training and culture, threat intelligence gathering arrangements, monitoring and analysing the threat intelligence received vis-à-vis the situation obtaining in banks, information sharing arrangements (among peer banks, with IDRBT/RBI/CERT-In), preventive, detective and corrective cyber security controls, vendor management and incident management & response are to be outlined.

Arrangement for continuous surveillance

6. Testing for vulnerabilities at reasonable intervals of time is very important. The nature of cyber-attacks are such that they can occur at any time and in a manner that may not have been anticipated. Hence, it is mandated that a SOC (Security Operations Centre) be set up at the earliest, if not yet been done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

IT architecture should be conducive to security

7. The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The same needs to be reviewed by the IT Sub Committee of the Board and upgraded, if required, as per their risk assessment in a phased manner. The risk cost/potential cost trade off decisions which a bank may take should be recorded in writing to enable an appropriate supervisory assessment subsequently.

8. An indicative, but not exhaustive, minimum baseline cyber security and resilience framework to be implemented by the banks is given in Annex 1. Banks should proactively initiate the process of setting up of and operationalising a Security Operations Centre (SOC) to monitor and manage cyber risks in real time. An indicative configuration of the SOC is given in Annex 2.

Comprehensively address network and database security

9. Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.

Ensuring Protection of customer information

10. Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, **irrespective** of whether the data is stored/in transit within themselves or with customers or with the third party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

Cyber Crisis Management Plan

11. A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. Considering the fact that cyber-risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate and hence needs to be revisited keeping in view the nuances of the cyber-risk. As you may be aware, in India, CERT-IN (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector. CERT-IN also have come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. CERT-In/NCIIPC/RBI/IDRBT guidance may be referred to while formulating the CCMP.

12. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. Banks are expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, banks should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

Cyber security preparedness indicators

13. The adequacy of and adherence to cyber resilience framework should be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including employees may also form a part of this assessment.

Sharing of information on cyber-security incidents with RBI

14. It is observed that banks are hesitant to share cyber-incidents faced by them. However, the experience gained globally indicates that collaboration among entities in sharing the cyber-incidents and the best practices would facilitate timely measures

in containing cyber-risks. It is reiterated that banks need to report all unusual cyber-security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank. Banks are also encouraged to actively participate in the activities of their CISOs' Forum coordinated by IDRBT and promptly report the incidents to Indian Banks – Center for Analysis of Risks and Threats (IB-CART) set up by IDRBT. Such collaborative efforts will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

Supervisory Reporting framework

15. It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents. Banks are required to report promptly the incidents, in the format given in Annex-3.

An immediate assessment of gaps in preparedness to be reported to RBI

16. The material gaps in controls may be identified early and appropriate remedial action under the active guidance and oversight of the IT Sub Committee of the Board as well as by the Board may be initiated immediately. The identified gaps, proposed measures/controls and their expected effectiveness, milestones with timelines for implementing the proposed controls/measures and measurement criteria for assessing their effectiveness including the risk assessment and risk management methodology followed by the bank/proposed by the bank, as per their self-assessment, may be submitted to the Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, Central Office not later than July 31, 2016 by the Chief Information Security Officer.

Organisational arrangements

17. Banks should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

Cyber-security awareness among stakeholders / Top Management / Board

18. It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing. It is well

recognised that stakeholders' (including customers, employees, partners and vendors) awareness about the potential impact of cyber-attacks helps in cyber-security preparedness of banks. Banks are required to take suitable steps in building this awareness. Concurrently, there is an urgent need to bring the Board of Directors and Top Management in banks up to speed on cyber-security related aspects, where necessary, and hence banks are advised to take immediate steps in this direction.

A copy of this circular may be placed before the Board of Directors in its ensuing meeting.

Yours sincerely,

(R.Ravikumar)
Chief General Manager
Encl: As above

Annex 1

Baseline Cyber Security and Resilience Requirements

An indicative but not exhaustive list of requirements to be put in place by banks to achieve baseline cyber-security/resilience is given. This may be evaluated periodically to integrate risks that arise due to newer threats, products or processes. Important security controls for effective cyber security as may be articulated by CERT-In also may be referred. Some of the key points to be kept in mind are:

a. In view of the growing technology adoption and potential threats, the role of IT Sub-committee may be reviewed; Board level involvement and guidance would set the right tone at the top.
b. It is important to endeavour to stay ahead of the adversary.
c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.
d. It is important to keep the vigil and to constantly remain alert.
e. While hardware devices and software applications may provide security, it is important to configure them appropriately.
f. Human resources are the key and ensure that they are provided with appropriate training. Communicate the security policy of the bank periodically.

Baseline Controls

1) Inventory Management of Business IT Assets

1.1 Maintain an up-to-date inventory of Assets, including business data/information including customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their business criticality. The banks may have their own framework/criteria for identifying critical assets.

1.2 Classify data/information based on information classification/sensitivity criteria of the bank

1.3 Appropriately manage and provide protection within and outside organisation borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within/outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

2) Preventing execution of unauthorised software

2.1 Maintain an up-to-date and preferably centralised inventory of authorised/unauthorised software(s). Consider implementing whitelisting of authorised applications / software/libraries, etc.

2.2 Have mechanism to centrally/otherwise control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block /prevent and identify installation and running of unauthorised software/applications on such devices/systems.

2.3 Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM/manufacturer/vendor for protection against well-known/well publicised/reported attacks exploiting the vulnerability patched, the banks must have a mechanism to apply them expeditiously following an emergency patch management process.

2.4 Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

3) Environmental Controls

3.1 Put in place appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats.

3.2 Put in place mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the bank.

4) Network Management and Security

4.1 Prepare and maintain an up-to-date network architecture diagram at the organisation level including wired/wireless networks;

4.2 Maintain an up-to-date/centralised inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network. The bank may consider implementing solutions to automate network discovery and management.

4.3 Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security;

4.4 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.5 Have mechanisms to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.

4.6 Have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

4.7 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

4.8 Establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

4.9 Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

4.10 Boundary defences should be multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network---based IPS and IDS. Mechanism to filter both inbound and outbound traffic to be put in place.

5) Secure Configuration

5.1 Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically,

5.2 periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including in Data Centres, in third party hosted sites, shared-infrastructure locations.

6) Application Security Life Cycle (ASLC)

6.1 Incorporate/Ensure information security across all stages of application life cycle.

6.2 In respect of critical business applications, banks may consider conducting source code audits by professionally competent personnel/service providers or have

assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

6.3 Secure coding practices may also be implemented for internally /collaboratively developed applications.

6.4 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

6.5 The development, test and production environments need to be properly segregated.

6.6 Software/Application development approach should be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.

6.7 Ensure that software/application development practices addresses the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

6.8 Consider implementing measures such as installing a “containerized” apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

6.9 Ensure that adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security team of the bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the bank.

7) Patch/Vulnerability & Change Management

7.1 Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

7.2 Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.

7.3 Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto

7.4 Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)

7.5 Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.

7.6 As a threat mitigation strategy, identify the root cause of incident and apply necessary patches to plug the vulnerabilities.

7.7 Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks are to be securely configured.

8) User Access Control / Management

8.1 Provide secure access to the bank's assets/services from within/outside bank's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other secure web protocols, etc.)

8.2 Carefully protect customer access credentials such as logon userid, authentication information and tokens, access profiles, etc. against leakage/attacks

8.3 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.

8.4 Implement centralised authentication and authorisation system or accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

8.5 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).

8.6 Implement controls to minimize invalid logon counts, deactivate dormant accounts.

8.7 Monitor any abnormal change in pattern of logon.

8.8 Implement measures to control installation of software on PCs/laptops, etc.

8.9 Implement controls for remote management/wiping/locking of mobile devices including laptops, etc.

8.10 Implement measures to control use of VBA/macros in office documents, control permissible attachment types in email systems.

9) Authentication Framework for Customers

9.1 Implement authentication framework/mechanism to provide positive identify verification of bank to customers.

9.2 Customer identity information should be kept secure.

9.3 Banks should act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

10) Secure mail and messaging systems

10.1 Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

10.2 Document and implement email server specific controls

11) Vendor Risk Management

11.1 Banks shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

11.2 Banks shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment.

11.3 Among others, banks shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

11.4 Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place.

11.5 Banks shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. Banks may necessarily enter into agreement with the service provider that amongst others provides for right of audit by the bank and inspection by the regulators of the country.

11.6 Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure/enabling resources may not physically be located in the premises of banks.

11.7 Further, banks have to adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

11.8 Banks shall thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

11.9 Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third party service providers

12) Removable Media

12.1 Define and implement policy for restriction and secure use of removable media/BYOD on various types/categories of devices including but not limited to workstations/PCs/Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use.

12.2 Limit media types and information that could be transferred/copied to/from such devices.

12.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access.

12.4 Consider implementing centralised policies through Active Directory or End-point management systems to whitelist/blacklist/restrict removable media use.

12.5 As default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.

13) Advanced Real-time Threat Defence and Management

13.1 Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

13.2 Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring.

13.3 Consider implementing whitelisting of internet websites/systems.

13.4 Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway

14) Anti-Phishing

14.1 Subscribe to Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

15) Data Leak prevention strategy

15.1 Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

15.2 This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

15.3 Similar arrangements need to be ensured at the vendor managed facilities as well.

16) Maintenance, Monitoring, and Analysis of Audit Logs

16.1 Consult all the stakeholders before finalising the scope, frequency and storage of log collection.

16.2 Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.

16.3 Enough care is to be taken to capture audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

17) Audit Log settings

17.1 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software , ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

18) Vulnerability assessment and Penetration Test and Red Team Exercises

18.1 Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the internet.

18.2 The vulnerabilities detected are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

18.3 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams.

18.4 Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Senior/Top Management.

18.5 Red Teams may be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

18.6 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

19) Incident Response & Management

Responding to Cyber-Incidents:

19.1 Put in place a fully effective Incident Response programme with due approval of the Board / Top Management.

19.2 Have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;

19.3 Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies.

Recovery from Cyber - Incidents:

19.4 Bank's BCP/DR capabilities shall adequately and effectively support the Bank's cyber resilience objectives and should be so designed to enable the bank to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

19.5 Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative & co-ordinated resilience testing that meet the bank's recovery time objectives.

19.6 Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders, reputation management. Adequate capacity

shall be planned and maintained, in consideration thereof. The following may be considered:

(a) Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.

(b) Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.

(c) Establish and implement systems to collect and share threat information from local/national/international sources following legally accepted/defined means/process

(d) Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.

(e) Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.

(f) Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

20) Risk based transaction monitoring

20.1 Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.

20.2 The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

21) Metrics

21.1 Develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

21.2 Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

22) Forensics

22.1 Have support/ arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by.

22.2 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

23) User / Employee/ Management Awareness

23.1 Define and communicate to users/employees, vendors & partners security policy/ies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cybersecurity risks and protection measures at their level.

23.2 Encourage them to report suspicious behaviour incidents to the incident management team.

23.3 Conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.)

23.4 Evaluate the awareness level periodically.

23.5 Establish a mechanism for adaptive capacity building for effective Cybersecurity Management. Making cyber security awareness programs mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year. (Recent and past cyber-attacks show, cyber adversaries are also targeting bank employees).

23.6 Board members may be sensitised on various technological developments and cyber security related developments periodically.

23.7 Board members may be provided with training programmes on IT Risk / Cyber-security Risk and evolving best practices in this regard so as to cover all the Board members atleast once a year.

24) Customer Education and Awareness

24.1 Improve and maintain customer awareness and education with regard to cybersecurity risks.

24.2 Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.

24.3 Educate the customers on the downside risk of sharing their login credentials / passwords etc. to any third party vendor and the consequences thereof.

Setting up and Operationalising Cyber Security Operation Centre (C-SOC)

Introduction

1 - Banking Industry in India has evolved technologically over the years and currently delivering innovative services to its customers. These services are delivered nonstop, round the clock and the customers access these services using Internet and Mobile Connectivity. Security of the financial transactions is of paramount importance and therefore the RBI has come out with guidelines from time to time addressing the security and operational aspects for specific applications and services.

2 - It is important and pertinent to look at specifically the Internet facing applications and services that are currently delivered and proposed to be delivered in the immediate future in the Banking Industry and come out with Cyber Security guidelines across the applications and services.

3 - Constant and Continuous monitoring of the environment using appropriate and cost effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is the urgent need for the Industry. Compliance to the Government guidelines that are put out periodically covering the cyber security policy, protecting critical information infrastructure and the Information Technology Act are of paramount importance. It is important to address the governance, technology, operational, outsourcing and legal issues while setting up the Cyber Security Operations Centre.

4 – Issues that need to be kept in mind while setting up the CSOC is given below. These are indicative but not exhaustive.

Governance Aspects:

- Top Management/Board Briefing on Threat Intelligence
- Dashboards and oversight
- Policy, measurement and enforcement (key metrics, reporting structure, define what is to be reported)
- Informing stakeholders , stakeholder participation

Cyber SoC: Points to be considered

1 - Conventional or Traditional Security systems have always focussed on preventive approaches over the years and are reactive in nature. They are in a position to address the concerns regarding known attacks. It is to be noted that the threat landscape has changed significantly in the recent past and therefore the approach and methodology required to be put in place has to necessarily take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero day attacks and attacks for which signatures are not available have to be kept in mind.

2 - The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.

3 - The systems that are implemented currently to monitor the security operation takes into account collection of the logs from each one of the point products deployed, storing and processing of the logs, correlation through appropriate SIEM tools, continuous monitoring of SIEM screens and finding the anomalies, if any and raising the alarms.

4 - The systems that NEED to be put in place as a part of the Cyber SoC requires the following aspects to be addressed.

- Methods to identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types.
- Incident investigation, forensics and deep packet analysis need to be in place to achieve the above.
- Dynamic Behaviour Analysis. – preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC)
- Analytics with good dash board, showing the Geo-location of the IP’s
- Counter response and Honeypot services

Expectations from SOC:

- Ability to Protect critical business and customer data/information, demonstrate compliance with internal guidelines, country regulations and laws
- Ability to Provide real-time/near-real time information on and insight into the security posture of the bank
- Ability to Effectively and Efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
- Ability to assess threat intelligence and the proactively identify/visualize impact of threats on the bank
- Ability to know who did what, when , how and preservation of evidence
- 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.

Key Responsibilities of SOC could include:

- Monitor, analyze and escalate security incidents
- Develop Response - protect, detect, respond, recover
- Conduct Incident Management and Forensic Analysis
- Co-ordination with contact groups within the bank/external agencies

5 - Building blocks for the Cyber SoC:

TECHNOLOGY ISSUES:

First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory

requirements. Clear understanding of the service delivery architecture deployed by the Bank to deliver innovative customer services will enable identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required.

Second step is to have security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations

Third step is to look at deep packet inspection approaches which are currently implemented using the UTM solutions that deliver wire speed performance with on the fly deep packet inspection.

Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements

It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability.

Need to think through by appropriately designing the

- SIEM architecture & use cases
- Log types and logging options (data sources, integration into SIEM)
- Integration of various log types and logging options into the 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.
- Technology for improving effectiveness and efficiency (tracking of metrics, analytics, scorecards, dashboards, etc.)

PROCESS RELATED ASPECTS:

One of the key aspects that require attention while designing the CSC is to understand the process to be followed to identify the root cause of a security breach and further steps to mitigate such attacks in future.

Incident Management

Problem management processes with reference to security operations Vulnerability and Patch Management Security risk management Availability management Computer forensics and response management are the key metrics that need to be well understood and architectured while configuring the solution.

PEOPLE RELATED ISSUES:

CSC is managed and monitored by competent and capable staff round the clock and therefore it is important to look at a suitable structure for this requirement.

The Level 1 monitoring by adequately trained staff working round the clock is the first step. They need to have training and product/ vendor certification to handle the tasks efficiently.

Level 2 deals with highly trained staff in specific areas of network, data security, end point security etc. to address the requirements especially while carrying out the root cause analysis as well as suitable corrective steps.

Level 3 staff are called the SoC analysts. They have profound knowledge of security, perform deep packet analysis, collection of IOC, forensic knowledge for collection of evidence, malware reverse engineering and write custom scripts whenever required.

It is to be noted that all the staff involved in the above exercise need to have a good knowledge of the products and services deployed by the respective Bank.

- Banks need to seriously consider practical ways of tackling the following issues when it comes to hiring and managing staff/people for SOC. It is not any other function in the bank. There has to be a different approach

because such personnel with required skill sets that are hard to find and retain.

- Staffing of SOC – is it required to be 24x7x365, in shifts, business hours only….etc.
- Model used - Finding staff with required skills /managed service provider with required skill set
- Training own staff/training of staff by service provider
- Appropriate compensation/incentives to retain trained staff /staff with required skill set
- Metrics to measure performance of SOC
- Ensuring scalability and continuity of staff through appropriate capacity planning initiatives

EXTERNAL INTEGRATION:

While delivering services to the customers of the Bank, several stake holders are involved directly or otherwise. They do have experience which could be very useful. For example the threat intelligence feeds from various sources may be provided by the product vendors and other major players in the technology landscape. Security information feeds from other Banks in particular and the financial ecosystem in general will be quite useful.

Cyber response cells, CERT-In and telecom service providers of the Bank may add value to the discussions based on the happenings in the Industry at large.

IDENTIFYING A SUITABLE MODEL FOR IMPLEMENTATION:

Some of the decisions which have to be taken upfront is to look at BOO or the Outsourcing model. It is difficult to reverse this decision post implementation and therefore it is important.

- Should the SoC be in-house or outsourced?
- Should it address only the Internet facing environment or the complete IT infrastructure?

- Does each Bank need to set up independently or should we look at the consortium based approach?
- Do we need to keep in mind the Bank's risk posture?

Points to keep in mind while planning for SOC in view of

(a) Specialized skill set requirements of operating and managing a SOC,

(b) Difficulty in finding experienced staff,

(c) Time consuming and expensive trainings,

(d) Designing of suitable compensation strategies,

(e) difficulty of retaining staff due to continual need for updated training, lack of adequate career path options, and overstretching ,

(f) Resource requirements pertaining to other supporting functions such as (i) system administration of systems facilitating SOC operations such as SIEM/dashboard/reporting/workflow/case management systems, etc., (ii) receiving, integrating and using threat intelligence, (iii) implementing communication strategy, (iv) Supervision/ management of SOC staff/personnel, (v) meeting compliance requirements of regulators/laws/regulations

Template for reporting Cyber Incidents

1. **Security Incident Reporting (SIR) to RBI (within two to 6 hours):**
2. **Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):**

Basic Information	
1. Particulars of Reporting:	
• Name of the bank	
• Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident:	
• Date and time of incident detection	
• Type of incidents and systems affected (i) **Outage of Critical IT system(s)** (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.) (ii) **Cyber Security Incident** *(e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web*	

defacement, etc.)? ***[Please complete Annex]*** (iii) **Theft or Loss of Information** *(e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)?* (iv) **Outage of Infrastructure** *(e.g. which premises-DC/Central Processing Units, branch, etc., power/utilities supply, telecommunications supply,)?* (v) **Financial** *(e.g. liquidity, bank run)?* (vi) **Unavailability of Staff** (e.g. number and percentage on loss of staff /absence of staff from work (vii) **Others** *(e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?*	
• What actions or responses have been taken by the bank at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment(examples are given but not exhaustive):	
• Business impact including availability of services – Banking Services, Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	

• Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc.	
• Regulatory and Legal impact	
4. Chronological order of events:	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	
• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such	

measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution_____ (DD/MM/YYYY).	
•	
•	
•	

Note: All fields are REQUIRED to be filled unless otherwise stated.

CYBER SECURITY INCIDENT REPORTING(CSIR) FORM	
General Information	**Report No:**

1. Contact Information: *(Please provide if different from what is reported in Basic Information above)*

Name of bank:

Name of the person reporting and Designation:

Department

Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

- For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3, X.4, etc. where X is the Report No.
  Update No: Click here to enter text.

3 What severity is this incident being classified as?

Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the bank's network / critical system(s) or a combination of them at risk	

Information about the Incident

4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

(Please specify in Indian Local Time (+5.30 GMT))

Reported to RBI - Date: Click here to enter a date.

Reported to CERT-IN Date: Click here to enter a date.

Reported to NCIIP Date: Click here to enter a date.

Reported to ----mention the name of agency Date: Click here to enter a date.

5. Types of Threat/Incident

((Please select more than one, as applicable)

☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)

☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access

☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage

☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

☐ Other: Click here to enter text.

6. Is this incident related to another incident previously reported?

Choose an item.

- If “Yes”, provide more information on how both incidents are related. Click here to enter text.
- Please provide the reference no. of the previously reported incident.

Ref no: Click here to enter text.

Incident Details

7. Please provide details of the incident in the box below.

- When was the incident first observed/sighted/detected?
  Click here to enter a date.

- How was the incident first observed/sighted/detected?
  Click here to enter text.

- Who observed?

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (*Tick 'one' checkbox for each column*)

Customer Service Delivery	(Loss of) Sensitive Information	Public Confidence and Reputation
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact

☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?

Choose an item.

- If "Yes", please provide more details.

Click here to enter text.

Incident Status

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? *(Tick 'checkbox' if unknown)*

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? *('NIL' OR 'NA' if unknown)*

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

Click here to enter text..

16. Is chain of custody maintained?

17. Has the bank filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

: Attack Vectors

E1. Did the bank locate/identify IP addresses**, domain names, related to the incident**

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies
