CORRIGENDUM TO THE BANK'S RFP NO. NHB(ND)/AAD/A10563/2019 DATED: SEPTEMBER 23, 2019

Please refer to the Bank's RFP dated: September 23, 2019, regarding engagement of Cyber Security Consultant, followed by pre-bid queries received from the bidders and pre-bid meeting held on October 03, 2019 at Bank's Head Office. In this regard, we request the bidders to be guided by the following table for amendments in the existing clauses. Other terms and conditions of the RFP shall remain same.

Clause. No.	Existing Clause	Amended clause
1.3	Last date and time for receipt of Bidding Documents – 21.10.2019 by 1800 hrs	Last date and time for receipt of Bidding Documents – 31.10.2019 by 1800 hrs
1.5	Date and time of opening of Technical Bid – 22.10.2019 by 1500 hrs	Date and time of opening of Technical Bid – 01.11.2019 by 1500 hrs
5 (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. Timeline : 5 weeks	Setting up of SOC The vendor will study the existing infrastructure of the Bank along with CSITE, RBI guidelines w.r.t. setting-up of C-SOC and prepare the RFP for selection consultant for the Bank. The RFP must be acceptable to National Housing Bank. The vendor would be responsible for evaluation of tender bids and would present their evaluation sheets before the Committee in coordination with All Audit Department (AAD). The work of the vendor would come to an end after on-boarding of the Consultant for setting up CSOC. The timeline for completion of RFP shall be 4 weeks from the acceptance and approval on Cyber Security Framework by the Bank. The timeline for evaluation of tender bids and submission of detailed evaluation sheets to the Committee in coordination with AAD would be 1 – 2 weeks from the date of opening of technical bids.
MEC 1	The Bidder must be an ISO	The Bidder must be an ISO 27001 certified

	27001 certified organization and should be a Private Limited of Limited Company	organization and should be a Private Limited, Limited or LLP firm
MEC 4	The bidder Company should have at-least 25 qualified Information Security / Cyber Security professionals (DISA/CISA/CISM/CDAC/ CEH) in their payroll.	The bidder Company should have at-least 25 qualified Information Security / Cyber Security professionals (DISA/CISA/CISM/CDAC/ CEH/ISO 27001 certified) in their payroll.
7.12.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	**7.12 Earnest Money Deposit (EMD) Request for Proposal:** All the responses must be accompanied by a refundable interest free security deposit of Rs. One Lac only (Rs. 1,00,000/- only), and RFP Cost of Rs. Ten Thousand (Rs. 10,000/-) by way of an e-payment in favour of National Housing Bank. The MSMEs having valid certificate issued by appropriate authority as defined under MSME Act 2006 and Public Procurement Policy, 2012 as Service Enterprises are exempt from depositing EMD and RFP Cost, provided they meet the following criteria: • The MSE's Bidder to note and ensure that nature of services and goods/items manufactured mentioned in MSE's certificate matches with the nature of the services and goods /items to be supplied as per Tender. • Traders/resellers/distributors/authorized agents will not be considered for availing benefits under PP Policy 2012 for MSEs as per MSE guidelines issued by MoMSME. • The registration certificate issued from any one of the above agencies must be valid as on Bid closing date of the tender. Bidder shall ensure validity of

		registration certificate in case bid closing date is extended.
		• The MSEs who have applied for registration or renewal of registration with any of the above agencies/bodies, but have not obtained the valid certificate as on close date of the tender, are not eligible for exemption/preference. For Bank Account details, please refer to Bank's 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.	The clause stands deleted.

	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.	
10.3	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	The service provider shall be paid as under: • 25% of the contract value on commencement of project in lieu of a PBG of the equivalent amount. • 35% of the contract value on submission of Cyber Security Policy & Cyber Crisis Management Plan and after its acceptance by the Bank • 20% of the contract value on submission of RFP for selection of consultant for setting up CSOC acceptable to the Bank • 20% of the payment after on-boarding of CSOC consultant.
New Cl (5.1)	Details on nos. of servers etc as indicated at Sr. No. 4 of the first table	The brief on IT Infrastructure of the Bank is given at Annexure – XVIII.

-Dy. General Manager
AAD

1. **Brief overview of Bank's IT Infrastructure**

NHB has centralized setup with DataCenter [DC] at New Delhi and Disaster Recovery [DR] Site at Mumbai. All applications are hosted at DataCentre, New Delhi and are accessed by all offices/ locations over MPLS WAN/ Internet. NHB at present has MPLS connectivity between Delhi, Mumbai & Other offices as under:

A. Wide Area Network (MPLS)

Presently NHB has MPLS connectivity between New Delhi, Mumbai & Regional Representative offices (RROs) as under. MPLS services are in managed mode.

S. No.	Location	Bandwidth
1.	New Delhi	34 Mbps
2.	Mumbai	16 Mbps
3.	RROs	1 Mbps

Presently Bank has four RROs at Ahmedabad, Bengaluru, Hyderabad and Kolkata.

B. Local Area Network

At New Delhi and Mumbai offices, the LAN is based on Layer 3 and Layer 2 switches. The switches used at the locations are manageable. All switches are property of NHB and are under Warranty/ AMC with respective vendors.

• At Delhi and Mumbai, Bank has deployed Cisco series switches

• At Delhi and Mumbai, Bank has installed Cisco ASA Firewalls.

• Other offices are connected to Head office over MPLS. The offices access Bank's hosted IT services over MPLS. MPLS network as well as the premises MPLS equipment is managed by present MPLS connectivity provider.

C. **Applications/Internet/Intranet etc.**

- Bank has setup Domain Controller (DC) & ADC for managing its environment.
- Bank has implemented SAP ERP system for most of its business operations.
- Mailing solution (MS Exchange) is available in high availability mode (DAG) with two primary servers at DC Site and one secondary server at DR site. Users at Delhi office access the corporate mail through LAN on MS Outlook. Other offices access the corporate mail over MPLS. Email service is also accessible for all NHB officials through Outlook Web Access (OWA) over Internet.
- Internet dedicated bandwidth from two different service providers are available at Delhi and Internet broadband is available at Mumbai. The bandwidths are used for Internet browsing and other web based services.
- NHB at its Delhi Office has implemented proxy server with web caching, web content filtering integrated with Active Directory at DC for user authentication and controlling user Internet access. In addition to this Bank has implemented Cisco ASA Firewall and Antivirus solution for security.
- NHB has SSL VPN Gateway to enable its employees to connect to IT services hosted in its Data Centre.
- APC Central log management solution is implemented at DC, New Delhi, to capture & deliver system logs for critical devices/ servers, in lucid manner to administrators.
- Bank uses services like NewsWire 18, Reuters at its treasury department to keep a tab on development happening in financial and treasury market.

D. **Website/Portals**

- Bank has its website (https://nhb.org.in): The website provides important information pertaining to various activities of the Bank. Besides, there are some portals also for different purposes like RESIDEX, CLSS, GRIDS etc.

E. **Infrastructure at Head Office, New Delhi**

Servers	Nos.
1. Servers - on Windows 2008/ 2012 platform - including SQL Server/ Exchange Server/SAP Servers and others	116

PCs	Platform	Nos.
1. Client Machines on LAN	Windows Vista/ 7/Windows 8/10	193
2. Laptops/Mobile Computers	Windows 7/8/10	114

F. **Infrastructure at Mumbai Regional Office**

Servers	Nos.
1. Servers - on Windows 2008/2012 platform - including SQL Server	16

PCs	Platform	Nos.
1. Client Machines on LAN	Windows XP/8/10	11
2. Stand-alone PCs	Windows 8	2
3. Laptops/Mobile Computers	Windows 7/8/10	7