राष्ट्रीय अवसंरचना वित्तपोषण और विकास बैंक (नैबफिड)

National Bank for Financing Infrastructure and Development (NaBFID)

(संसद के अधिनियम के माध्यम से स्थापित एक अखिल भारतीय पिकास पित्तीय संस्था)

(An All-India Development Financial Institution established through an act of Parliament)

REQUEST FOR PROPOSAL FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF A CLOUD BASED VULNERABILITY MANAGEMENT SOLUTION AND DEPLOYMENT OF ON-PREMISE RESOURCES FOR SECURITY TESTING

Ref: NaBFID / IS / RFP /10 dated March 30 ,2026

GEM Bid Ref No: GEM/2026/B/7403532

(Bidding Through GEM Portal Only)

Issuing Office and Address:
National Bank for Financing Infrastructure and Development (NaBFID)
15th Floor, Tower A
The Capital
Bandra-Kurla Complex, Bandra (East)
Mumbai – 400051

For queries, please contact:
Email id: rfp@nabfid.org

Last date and time for submission of bids
April 21, 2026, up to 16:00 hrs.

Schedule of Events

	Particulars	Remarks
1	Coordinates for correspondence	Email ID: rfp@nabfid.org Address: National Bank for Financing Infrastructure & Development (NaBFID) The Capital, A wing, 15th floor – 1503, G block,BKC,Bandra , Mumbai - 51
2	Bid Document Availability including changes / amendments, if any, to be issued	Bid document may be downloaded from NaBFID's official website – www.nabfid.org or from the GeM portal.
3	Pre-Bid Meeting	**April 6, 2026 at 4:00 PM** (Online– Via Teams Meeting)
4	Last date for requesting clarification/Queries	Up to 4.00 PM on April 10, 2026 All communications regarding points / queries requiring clarifications shall be given by email to rfp@nabfid.org
5	Last date and time for Bid submission	Up to 4.00 PM on April 21, 2026
6	Address for submission of Bids	Through GeM portal
7	Date and Time of opening of Technical Bids	4.30 PM on April 21 , 2026 *Note- Authorized representatives of Bidders may be present during the opening of the Bids. However, Bids would be opened even in the absence of any or all the Bidder representatives.*
8	Announcement of shortlisted bidders	Shall be communicated subsequently
9	Earnest Money Deposit (EMD)	Rs. 3,00,000/- (Rupees Three Lakhs only) in the form of Demand Draft/Bank Guarantee in favour of National Bank for Financing Infrastructure and Development payable at Mumbai, India. Note: *Earnest Money Deposit (EMD) should be enclosed on a separate cover and should not be included in technical or commercial price bid.*

Contents

1. Objective of the RFP 5
2. Disclaimer 5
3. Definitions 6
4. Eligibility Criteria 6
5. Skill set & Experience requirements for resources. 6
6. Scope of Work 8
7. VAPT scope 19
8. Tools Required 20
9. Deliverables & Implementation Timelines 20
10. Cost of bidding 21
11. Language of bid 21
12. Services and Adherence to Standards 21
13. Clarification and Amendments on RFP / Pre-Bid Meeting: 21
14. Contents of Bid Document 22
15. BID Preparation & Submission 22
16. Period of Bid Validity 22
17. Bid Integrity 22
18. Bid Security/ EMD (Refundable) 22
19. Amendment of Bidding Documents 23
20. Authorization to Bid 23
21. Technical & Commercial bids 23
22. Rejection of Bid 25
23. RFP Clarifications / Bidder's queries 25
24. Technical Bid Evaluation 25
25. Evaluation Methodology 26
26. Awarding of contracts / Projects 27
27. Penalties & Payment Terms 27
28. Right to Audit 29
29. Sub-Contracting 29
30. Limitation of Liability 30

31. Confidentiality 30
32. Delay in Service Provider's Performance 30
33. Service Provider's Obligation 30
34. Liquidated Damages 31
35. Termination for Default 31
36. Force Majeure 32
37. Disputes / Arbitration (Applicable only in case of successful bidders) 32
38. RFP Ownership 33
39. Tender/RFP Cancellation 34
Annexure A 35
Annexure B 37
Annexure B1 39
Annexure B2 40
Annexure C1 41
Annexure C2 43
Annexure D 46
Annexure E 50
Annexure F 51
Annexure G 52
Annexure H 53
Annexure I 54
Annexure J 63
Annexure K 64
APPENDIX I 65
APPENDIX II 72

1. Objective of the RFP

National Bank for Financing Infrastructure and Development (NaBFID) a body corporate constituted under The National Bank For Financing Infrastructure And Development Act, 2021 having its office at A-1503, The Capital, G-Block, Bandra-Kurla Complex, Bandra (East), Mumbai – 400051 and with one branch office at New Delhi.

The purpose of this Request for Proposal (RFP) is to select a qualified bidder for the supply, implementation, and ongoing operation & maintenance of a cloud-based Vulnerability Management (VM) solution through a certified OEM partner. The selected bidder will also be responsible for deploying security resources to perform periodic Vulnerability Assessments (VA), Compliance Scanning (as per Bank SCD), Penetration Testing (PT), Application, Mobile, and API Security Testing, and Container Vulnerability Scanning, in accordance with the scope and requirements specified in this RFP.

2. Disclaimer

a) The information contained in this RFP or information provided subsequently to Bidder(s) whether verbally or in documentary form / email by or on behalf of NaBFID, is subject to the terms and conditions set out in this RFP.
b) This RFP is not an offer by NaBFID, but an invitation to receive responses from the eligible Bidders.
c) The purpose of this RFP is to provide the Bidder(s) with information to assist with the preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advice / clarifications. NaBFID may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.
d) NaBFID and its employees make no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.
e) NaBFID also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever, caused arising from reliance of any Bidder upon the statements contained in this RFP.
f) The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respects will be at the Bidder's risk and may result in rejection of the Bid.
g) NaBFID reserves the right to reject all or any the Proposals without assigning any reason thereof and to restrict the list of Bidders to any number as deemed suitable, if too many applications/Proposals are received satisfying the basic pre-qualification criteria.

h) NaBFID also has the right to reject all the applications and to go in for a readvertisement without assigning any reason thereof.

3. Definitions

In this connection, the following terms shall be interpreted as indicated below:

a) "NaBFID" means the National Bank for Financing Infrastructure and Development as incorporated under the National Bank for Financing Infrastructure and Development (NaBFID) Act, 2021.
b) "Bidder" means an eligible entity/firm, submitting the Bid in response to this RFP.
c) "Bid" means the written reply or submission of response to this RFP.
d) "The Contract" means the agreement entered into between NaBFID and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
e) "Selected Bidder / Vendor / Service Provider / Consultant" is the successful Bidder found eligible as per eligibility criteria set out in this RFP.
f) "Services" means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include provision of technical assistance, training, certifications, auditing and other obligations of Bidder covered under this RFP.
g) "Purchase Order" means an official document issued by NaBFID to the selected bidder awarding the contract to the Selected Bidder.
h) "Eligibility Bid" means a bid document to identify Bidders who meet the minimum criteria set out by NaBFID to become eligible for the technical Bid.
i) "Eligibility Criteria" means the criteria listed in Annexure – B on the achievement of which a Bidder becomes eligible for technical Bid.
j) "Non-disclosure Agreement or NDA" means a contract by which NaBFID and the Bidder agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.
k) "Scheduled Commercial Bank" means all banks are included in the second schedule to the Reserve Bank of India Act, 1934.
l) "Manpower Services" means all services, scope of work and deliverables to be provided by the Bidder as described in the RFP.

4. Eligibility Criteria

Only those Bidders fulfilling the eligibility & Technical Compliance sheet mentioned in **Annexure-B & Annexure-I** (respectively) should respond to the RFP. Offers received from the vendors who do not fulfil any of the following eligibility criteria are liable to be rejected. A Bidder is not permitted to submit more than one Bid.

5. Skill set & Experience requirements for resources.

Details of minimum educational qualifications, skill sets, and experience required for various levels of resources (if required to manage the project) are as given below.

Level 1 or Qualified SME as per requirement	**Educational Qualifications:** Graduation **Experience:** The bidder shall assign one full-time L1 resource dedicated on-premises **for execution of Vulnerability Assessment (VA) activities and CIS Benchmark-based configuration compliance assessments and for creation of SCDs(Secure configuration Document)** throughout the engagement period. For other activities (Penetration Testing, Container Scanning, API Security testing, Application & Mobile Security Testing & Static Application Security Testing(SAST)), the bidder shall provide qualified SMEs with suitable experience as mentioned below and in accordance with the frequency and schedule specified in Section 7 of this RFP. Each deployed **Subject Matter Expert (SME)** resource must meet the following minimum experience requirements according to the activity: **VA:** Minimum 2 years of hands-on experience in conducting Vulnerability Assessment in BFSI sector across diverse environments (on-premises, cloud, and hybrid). (Certificate Required: CEH) **Network PT:** Minimum 4 years of experience in BFSI sector in conducting internal and external network penetration tests, including exploitation. (Certificate Required: CEH Masters or eJPT or OSCP) **Application PT:** Minimum 4 years of experience in BFSI sector in performing black-box and grey-box dynamic application security testing(DAST) of web applications in line with OWASP Top 10 and SANS Top 25 standards. (Certificate Required: Burp Suite Certified Practitioner or CEH Masters or eJPT or OSCP) **API security testing:** Minimum 4 years of experience in performing black-box and grey-box DAST testing of APIs in BFSI sector in line with OWASP Top 10 and SANS Top 25 standards. (Certificate Required: Burp Suite Certified Practitioner or CEH Masters or eJPT or OSCP) **Mobile Security Testing:** Minimum 4 years of experience in performing black-box and grey-box DAST testing of mobile applications in BFSI sector in line with OWASP Top 10 and SANS Top 25 standards. (Certificate Required: Burp Suite Certified Practitioner or CEH Masters or eJPT or OSCP) **Compliance Scan:** Minimum 2 years of experience in performing compliance scan as per CIS benchmarks in BFSI sector , using both automated tools and manual assessment techniques (Certificate Required:CEH) **Container Scans:** Minimum 2 years of hands-on experience in deploying, configuring, and managing container security and

	vulnerability scanning solutions, including performing vulnerability assessments and configuration security scans of container images, running workloads, and registries on platforms such as Red Hat OpenShift, OpenShift Kubernetes Engine (OKE), and similar container orchestration environments. **SAST Scans:** Minimum 4 years of experience in performing SAST testing of applications in BFSI sector in line with OWASP Top 10 and SANS Top 25 standards. (Certificate Required: Burp Suite Certified Practitioner or CEH Masters or eJPT or OSCP)

Note: ***Onboarding resources will be at the absolute discretion of the bank. Bank may place the order to the selected bidder with / without facility management resource, at its discretion.***

6. Scope of Work

The Bank plans to implement the cloud-based Vulnerability Management (VM) solution through a certified OEM partner, and to seek one dedicated security resource to manage the cloud VM solution, perform periodic Vulnerability Assessments (VA), Compliance Scanning (as per CIS Benchmarks) and creation of Security Control Documents (SCDs).

For other activities, periodic resources are required (frequency of which is specified in section 7)to perform Penetration Testing (PT), Application, Mobile, and API Security Testing, and Container Vulnerability Scanning based on the following scope (not limited to):

6.1 Tool Deployment & Licensing

1. Provision of a SaaS-based Vulnerability Management solution for up to 500 assets through a certified OEM partner
2. The license shall be procured in the name of the Bank and remain valid for a period of three (3) years.
3. All licensing, subscription, and operational costs shall be borne by the Bank.
4. The bidder shall ensure smooth tool onboarding, configuration, and operation throughout the contract period.

6.2 Tool Capabilities

The proposed VM tool shall:

1. Perform Vulnerability Assessments and Compliance Scans (SCD baseline scans) for all types of assets (servers, network devices, storage, etc.) under a single license.
2. Have capability of scanning container workloads under a single license or by taking additional licenses and to integrate with proposed Vulnerability management solution for management and dashboarding purpose.
3. Support both authenticated credential-based scanning and unauthenticated scanning.

4. Provide CVE-to-detection mapping, CVSSv2/v3 scoring, and correlation with CISA KEV and MITRE ATT&CK frameworks.
5. Support role-based access control (RBAC), asset tagging, and automated report generation.
6. Detailed capabilities along with mandatory requirements are mentioned in the technical & functional requirement section.

6.3 Initial Setup & Configuration

The selected bidder shall be responsible for:

1. deployment, configuration, and management of the VM tool within the Bank's environment.
2. Fine-tune configurations to align with the Bank's security policies, infrastructure, and asset inventory.
3. Prepare and hand over configuration and deployment documentation, including credentials management, asset onboarding process, and scanning workflows.

6.4 Resource Deployment

The bidder shall deploy one (1) full-time dedicated on-site L1 resource for a period of three (3) years to perform Vulnerability Assessment (VA) activities and CIS Benchmark-based configuration compliance assessments. The dedicated resources shall be stationed at the Bank's premises throughout the engagement period and shall act as the Single Point of Contact (SPOC) for the engagement. For activities other than VA and CIS configuration assessments, including but not limited to Penetration Testing (PT) and other specialized security assessments, the bidder shall provide qualified SMEs in accordance with the frequency and schedule defined in Section 7. All deployed resources must meet the minimum experience and qualification requirements relevant to their assigned roles and activities.

6.5 Resource Responsibilities

6.5.1 Vulnerability Assessment (VA) & Configuration Scans

1. Conduct VA for up to 500 assets (servers, network devices, containers, etc.) using the Bank's licensed VM tool.
2. Perform half yearly authenticated scans covering operating systems (Windows, Linux, Unix), network devices (routers, switches, firewalls etc), security devices (SIEM,PIM,EDR,WAF etc).
3. To perform container-based vulnerability assessment of images and running containers and the underlying OS.

4. Manage end-to-end VA activities, including troubleshooting, authenticated scanning, connectivity resolution with various vendors and Bank Teams, and customized report generation.
5. Conduct compliance scans against Bank defined SCDs and generate compliance deviation reports.
6. To develop Secure Configuration Documents (SCDs) and corresponding audit policies in line with industry-recognized best practices and standards such as CIS Benchmarks, DISA STIGs, OEM hardening guides, or other equivalent and widely accepted security frameworks.
7. Provide technical guidance and consultation for remediation of identified vulnerabilities.
8. Conduct post-remediation verification scans as soon as confirmation comes from vendor for closure and submit compliance closure reports in the Bank's prescribed format.
9. To coordinate all other security testing activities(VA,PT,SAST,DAST etc) with various bank vendors and bank teams.
10. To perform security assessments of the Bank's container orchestration platforms, using VM tool procured through this RFP. The assessment shall include vulnerability scanning and configuration review of clusters, nodes, container images, and workloads, covering RBAC, pod/container security, network policies, secrets management, and cluster controls in accordance with container security best practices.

6.5.2 Penetration Testing (PT)

The vendor should conduct PT for identified Ips/URLs to get a 'hacker's eye' view of NABFID's network to identify security holes that could be exploited by remote attackers. It should not be limited to information pilferage, denial of service, password cracking, brute force attack etc. The detailed scope is given below:

A. External PT

1. Conduct scoping meetings to define IPs, URLs, and network ranges for testing.
2. Perform public IP discovery and scanning once every six (6) months to identify live IPs.
3. Enumerate services (HTTP/HTTPS, SSH, FTP, etc.) running on identified IPs.
4. Conduct black-box network penetration testing on live IPs, including:
    - Port scanning and service enumeration
    - Banner grabbing and fingerprinting
    - Vulnerability exploitation simulation
5. Conduct application-level PT (if a web/API service is identified on a running port) in accordance with OWASP Top 10 and SANS Top 25 guidelines.

6. Conduct device-level PT for network devices (e.g., routers, switches, firewalls) focusing on configuration weaknesses, known vulnerabilities, and exploitable services.
7. Re-test vulnerabilities identified during PT exercises upon Bank's request.
8. Testing shall be conducted externally, with prior approval of testing tools, ensuring no disruption to production.

B. Internal PT

1. Perform internal IP/URL-based PT on a requirement basis following the same approach as external PT.
2. Conduct testing securely within the Bank's internal environment with necessary approvals.

C. Application PT(Web, Mobile, API etc.)

1. Conduct grey-box or Blackbox PT for applications (web, mobile, API, thick/thin client) in UAT environments as per OWASP Top 10 and SANS Top 25 standards.
2. Provide detailed findings, exploit proofs (where allowed), and remediation recommendations as part of report.

6.5.3 Frequency & Reporting

1. VA& PT shall be conducted on half yearly basis.
2. Submit detailed VA & PT reports as per bank prescribed format including:
    - Detailed reports IP wise/URL wise/Application wise as per bank format.
    - To maintain consolidated VA & PT tracker (Vulnerability wise & IP wise) for all the IPs/URLs/Applications as per bank format and submit to bank on daily basis.
    - All the reports contain approach & methodology, Risk ratings, remediation steps, and recommendations.
    - Re-compliance reports after closure of vulnerabilities.
    - Monthly status reports.
    - Calculation and preparation of RBI KRI data and submit to bank on quarterly basis.

6.5.4 Additional Responsibilities

1. Identify security gaps, provide remediation measures, and recommend both tactical (short-term) and strategic (long-term) controls.
2. Assist in vulnerability remediation, revalidation, and submission of supporting evidence to confirm closure.

3. Provide technical consultation and expert guidance to mitigate identified vulnerabilities and strengthen overall security posture.
4. Coordinate with all relevant stakeholders of the Bank for smooth execution of VAPT activities, including resolution of issues such as network connectivity, authentication failures, and scan configuration errors.
5. Validate and report false positives with appropriate supporting evidence for Bank review and approval.
6. Present VAPT findings and status updates to the CISO and, when required, to the Board of Directors, through a qualified senior expert from the bidder's organization.

6.6 Security requirements for Cloud based VM solution

The OEM partner should submit the following documents related to security capability of OEM where the tool shall be deployed:

1. To submit latest SOC2 type 2 report of OEM to the bank on yearly basis.
2. To submit latest ISO 27001 certificate of OEM and partner both.
3. Based on various regulatory guidelines the OEM/ Bidder must provide the Software Bill of Material (SBOM) and Cryptography Bill of Material (CBOM) in the standard formats such as SPDX (Software Package Data Exchange), CycloneDX etc., as and when required by the Bank without any additional cost.
4. To perform & submit half yearly VA & PT closure reports of bank instance hosted in Cloud.
5. All vulnerability data (scan results, asset metadata, logs) should be stored and processed within India, or a region approved by the Bank and regulator. OEM to provide confirmation of data storage location and hosting provider details with relevant evidence.
6. Data must be encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent).OEM to provide encryption architecture and key management process.
7. OEM to provide confirmation that the Bank retains full ownership of data and that OEM acts only as a data processor. Data must not be shared with third parties without written consent.
8. OEM must support secure data deletion (e.g., NIST 800-88 compliant) on termination.
9. The Bank's scan data should be logically isolated (via tenant isolation or VPC segmentation).
10. OEM to support MFA, role-based access control (RBAC), and audit trails for all user actions.
11. OEM must perform continuous SOC monitoring and log correlation for its SaaS platform.

12. OEM should have an incident response plan and notify the Bank within 4 hours of any security incident as per CERT-IN guidelines.

13. Integrity Certificate as per bank prescribed format to be submitted.

6.7 General Requirements:

1. The solution must support seamless integration with the Bank's existing SIEM solutions (LogRythm, IBM Qradar & Gurucul etc) without any additional cost to the Bank.
2. The proposed solution should support the integration with Bank's ITSM solution (Freshservice) without any additional cost to the Bank.
3. The solution provider/ OEM must have certified against internationally recognized government and commercial standards - frameworks such as ISO27001, ISO 27701, ISO 27018, ISO 27017, AICPA SOC 2 Type 2, CSA - Star, NIST 800-63C, NIST 800-53, etc
4. The SOC 2 Type 2 audit reports & certificates of the proposed cloud-based solutions should be shared with the Bank on annual basis.
5. The proposed solution should comply with the Digital Personal Data Protection Act (DPDP) during the contract period. Any changes required will be carried out by the bidder with no additional cost to the Bank.
6. The proposed solution must have in-built data log retention of at least 1 year from for all components.
7. The selected bidder should provide training for the selected Bank officials on the proposed solutions without any additional cost to the Bank.
8. Bank, Regulators & bank authorized partners reserve the right to audit the OEM infrastructure where the bank tool is hosted.

6.8 Functional & Technical Requirements

There are certain requirements that are mandatory in nature, the remaining parameters are desirable as indicated below.

I. General Requirements

Sr No	Solution Capabilities	Mandatory/Desirable
1.	The solution must be a cloud-based SaaS platform hosted in India.	Mandatory
2.	Solution must support multi-user RBAC with SSO/SAML and MFA.	Mandatory

II. Asset Discovery and Inventory Management

Sr No	Solution Capabilities	Mandatory/Desirable
1.	Automatic discovery of known and unknown assets across on-prem, cloud, containers, and endpoints	Mandatory

2.	Give the user the flexibility to create dynamic tags basis on "asset name", "asset inventory", IP address and range, open ports, vulnerability, etc.	Desirable
3.	Must identify and tag software to either Commercial or Opensource software	Desirable
4.	Ability to view asset, software, ports, certificates, and vulnerabilities on a unified dashboard.	Desirable
5.	Ability to scan IPs simultaneously and the rest of the IP's /asset scheduled for scanning (in any site) to be able to put in the scanning queue and run automatically.	Mandatory
6.	The solution must support advanced query and search features for assets and vulnerabilities, including: • Elastic search-like query capability with filtering and sorting. • Ability to save and reuse queries for recurring analysis and reporting.	Desirable
7.	The solution must provide a customizable and interactive dashboard that allows users to: • Create and personalize dashboards based on asset search queries. • Convert clicks or filters into query-based views. • Drag and drop widgets for repositioning and layout customization. • Apply color coding to represent risk levels or categories (e.g., high, medium, low).	Desirable
8.	The dashboard must offer rich visualization and drill-down capabilities, including: • Multiple widget formats (pie charts, bar charts, value indicators, and list views). • Drill-down from summary views to detailed asset and vulnerability data. • Daily trend visualization within widgets for tracking changes over time. •Should be able to convert a query into a widget	Desirable

III. Vulnerability Management

Sr No	Solution Capabilities	Mandatory/Desirable
1.	Support for authenticated and unauthenticated scans for OS, databases, applications, and network & security devices.	Mandatory

2.	Should support authentication support but not limited to Linux, Windows, Network and Security devices (Checkpoint FW, Cisco, Cisco APIC Infoblox, Network SSH, Palo Alto FW, SNMP), Applications (Apache, BIND, Docker, HTTP, Jboss, MS IIS, Kubernetes, NGINX, Tomcat, Oracle Weblogic etc.), Databases (Azure MS SQL, Cassandra, IBM DB2, MariaDB, MongoDB, MS SQL, MySQL, Oracle, SAP HANA, PostgreSQL etc.), VMware for authentication	Mandatory
3.	Should support integration with authentication vaults - CyberArk PIM, CyberArk AIM, Thycotic, Beyond trust PBPS, Hashicorp, Azure Key, Arcon PAM, Liebeman ERPM, Wallix (WAB).	Mandatory
4.	Enables discovery of assets in the environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets.	Mandatory
5.	Gather detailed information, such as an asset's details, running services, installed software, and more and eliminate the variations in product and vendor names and categorize them by product families on all assets.	Desirable
6.	Must include CVE-to-detection mapping and CVSSv2/v3.	Mandatory
7.	The solution must leverage global threat intelligence frameworks such as MITRE ATT&CK to map vulnerabilities with corresponding tactics and techniques, thereby enabling threat-informed vulnerability prioritization and remediation planning.	Desirable
8.	The solution must enrich vulnerabilities with real-time threat indicators (RTIs) sourced from both internal and external feeds (e.g., CISA KEV, public exploits, malware associations, zero-day alerts, and active exploitation data). It should automatically tag vulnerabilities with contextual attributes such as *Actively Exploited, Easy Exploit, High Data Loss, Denial of Service, No Patch, Exploit Kit,* etc., to support risk-based remediation and improve visibility into real-world exploitation trends.	Desirable
9.	Allow risk scoring based on exploitability, business impact, and lateral movement potential.	Desirable
	Should have an automated way to "Ignore" vulnerabilities with easy tracking for exception management and/or false positives	Mandatory
10.	Support Static and Dynamic tagging for asset management, scanning and reporting	Desirable
11.	Should support out of box query/token for assets and vulnerabilities like threat hunting any asset with	Desirable

	vulnerability having remote code execution or ransomware associated to it	
12.	Integration with ITSM tools (e.g., ServiceNow) ,GRC archer and SIEM solutions through API.	Desirable
13.	Should support unlimited multiple sensors for inventory - virtual scanners, agents, container sensors etc for asset inventory.	Desirable
14.	Option to group the assets basis on OS, software, tags, last logged in user, created, last seen etc.	Desirable
15.	The solution must support agent-based, agentless, and hybrid scanning modes. Able to scan a host (wherever applicable) with agent and scanner both consuming only single license	Mandatory
16.	Must encrypt scan data in transit and at rest.	Mandatory
17.	Support custom and predefined reports (Executive, Technical, PCI, etc.) in PDF/CSV formats.	Mandatory
18.	Able to provide remediation suggestion in the scan reports	Mandatory
19.	The solution must be capable of tracking the status of each vulnerability across iterative scans, including its lifecycle state (e.g., new, existing, or reopened) to ensure accurate remediation tracking and trend analysis. It should also display key timeline details such as the initial date of discovery, last observed date, and closure verification date (where applicable).	Mandatory
20.	Auto updating & self managing scanners and agents	Mandatory
21.	Should have the ability to auto-eliminate superseding patches	Mandatory
22.	Should provide information if the vulnerability has a virtual patch available	Desirable
23.	Report generation through API	Desirable
24.	Have the capability for Automatic correlation between CVE and Patch KB	Mandatory
25.	Option to group the vulnerabilities basis on name, age, severity, cvss rating, vendor, vendor product name, OS, status, malware name, RTIs, Public exploit, exploit kit etc.	Desirable
26.	Schedule discovery/map scans and vulnerability scans and sent the notification before and after scan completion.	Mandatory
27.	The quoted license cost for the Vulnerability Management Solution shall be based on number of assets, where an asset shall be defined as a unique host or endpoint identified by a unique IP address, hostname, or agent installed on the system.	Mandatory

	The following shall be considered a single asset: • Server (Physical or Virtual) • Desktop / Endpoint • Network Device (Firewall, Router, Switch, Load Balancer) • Cloud Instance / VM Multiple services, open ports, applications, or domains running on the same host shall not be counted as separate assets. The solution must support agent-based and agentless scanning within the same license without additional cost.	
28.	The proposed Vulnerability Management Solution shall support unlimited vulnerability scans of assets for which licences are taken during the contract period. The license shall not restrict: • Number of scans • Number of scan schedules • Number of vulnerability signatures/plugins • Number of scanning policies • Number of scanning engines required within the licensed asset limit. The Bank may perform on-demand, scheduled, or continuous scanning without additional licensing cost.	Mandatory
29.	The proposed solution must support vulnerability scanning for on-premise and cloud environments including workloads hosted in public cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform without additional licensing cost within the asset limits.	Mandatory

III. Agent Security

Sr No	Solution Capabilities	Mandatory/Desirable
1.	Agent should provide a continuous view of assets for vulnerability management, configuration assessment, and asset inventory without the need for credential management, and firewall changes required by network scanner deployments.	Mandatory
2.	Agent's design should focus on "One Agent - Multiple Capabilities" which means same agent shall be performing inventory, vulnerability, configuration assessment, asset management (including security use cases), Software Composition Analysis (SwCA), Passive Sensing etc.	Desirable

3.	Solution should be able to merge the scan data from agent and scanner and provide a single instance for the vulnerability	Mandatory
4.	The agent shall be lightweight with a low CPU and memory footprint, designed for high-performance functionality. It should capture only delta changes in metadata and securely transmit them to the management server for centralized processing, analysis, reporting, and configuration management.	Mandatory
5.	Agent should be light weight, have a low CPU and memory footprint which shall bring the high-performance functionality of the agent & built in configurations for central management	Desirable
6.	Users shall be able to uninstall the agents which are not reporting to the management server automatically or manually from the UI	Mandatory
7.	Agent should be self updating and tamper resistant	Mandatory
8.	Lightweight, auto-updating agent supporting Agent-based detection (On prem) Agent Support Windows (client and server versions) Agent Support Linux and Unix Agent Support Mac OS Agent Support AIX Agent Support for ZLinux Agent Support for Solaris Agent Support for Gentoo Agent Support for ChromeOS	Mandatory

IV. Container Security

The bidder shall indicate any additional licensing requirements for the container security module, if applicable, which may be procured separately by the Bank based on necessity. The proposed module shall be from same OEM.

Sr No	Solution Capabilities	Mandatory/Desirable
1.	The proposed solution should be from same OEM and capable of scanning container workloads (with additional licenses if required) and integrate with the Vulnerability Management solution for unified reporting and dashboarding.	Mandatory
2.	The solution must provide end-to-end container security, including runtime protection, image scanning, and continuous vulnerability management for containers, images, and registries without requiring manual intervention.	Desirable
3.	The solution shall support clustered container orchestration environments like Kubernetes, OpenShift, Docker Swarm and managed services like AKS, ECS, EKS, OKE etc.	Mandatory

4.	Ability to scan directly into Red Hat Enterprise Linux CoreOS in Red Hat OpenShift, to identify vulnerabilities and manage risk at both RHCOS OS and container levels.	Mandatory
5.	Should support container security with scanning for images, registries (ECR, GCR, JFrog, etc.), and runtime workloads.	Mandatory
6.	The solution shall have the ability to do automatic discovery, Inventory of all the containers and images with all metadata.	Mandatory
7.	Support for Software Composition Analysis (SCA) and malware/secret detection in container images	Desirable
8.	The solution must have detailed vulnerability information like identification, analysis, CVSS score, remediation etc. for containers.	Mandatory
9.	The solution shall perform configuration and compliance checks on running containers, provide remediation for failed checks, and support exception management for approved deviations. It must support management of vulnerability, compliance, access, and audit controls in containerized environments.	Desirable

IV. Support and SLA

Sr No	Solution Capabilities	Mandatory/Desirable
1.	OEM / Bidder must provide 24x7 support through email and portal.	Mandatory
2.	Critical issue response time: ≤ 12 hours; Medium: ≤ 48 hours; Low: ≤ 3 business days.	Mandatory
3.	Availability of a Technical Account Manager (TAM) during the contract period from OEM.	Desirable

7. VAPT scope

Details of the assets & application along with scanning scope are mentioned in the table below. The bidder shall deploy one full-time resource for VA, compliance scan and vulnerability Scanning (Images & running containers) related activity as mentioned below in Sr.no 1 ,2 & 6. For the activities mentioned in Sr. No. 3,4,5 & 7, the bidder shall deploy additional Subject Matter Experts (SMEs) on a periodic basis at the Bank's premises as per the frequency defined below.

S.no	Scanning Type	Assets/Application Count	Frequency
1	VA using proposed VM tool	500 IPs	As and when required during contract period.

2	Compliance Scan as per Bank defined SCD Benchmarks using proposed VM tool	500 IPs	As and when required during contract period.
3	Network PT	50 IPs	Half yearly (Initial Scan + 2 Rescans)
4	Application PT as per latest OWASP top 10 & SANS Top 25	15 Applications	Yearly (Initial Scan + 2 Rescans)
5	API security testing as per latest OWASP top 10 & SANS Top 25	100	Yearly (Initial Scan + 2 Rescans)
6	vulnerability Scanning (Images & running containers) & configuration checks on Bank's container orchestration platforms using bidder standard tools or tools procure through this RFP.	6 worker nodes	As and when required during contract period.
7	Mobile PT as per latest OWASP top 10 & SANS Top 25	1	Yearly (Initial Scan + 2 Rescans)

8. Tools Required

For Vulnerability Assessment (VA) , compliance scan (Based on SCDs) & Container scan activities, the bidder shall be responsible for deploying, managing, and executing scans using the proposed cloud-based Vulnerability Management (VM) solution & container security module. For all other activities — including all types of Penetration Testing (PT), Source Code Review etc., as defined in the above scope, the bidder shall utilize their own licensed tools and utilities to perform the testing.

9. Deliverables & Implementation Timelines

- Supply of licenses for all the components mentioned in the scope.
- Implementation, Maintenance and Management of the solution for a period of 3 years, extendable for 2 more years.
- Product documents, including Solutioning documents, HLD, LLD
- Standard Operating procedures.
- OEM specific certified training & certification voucher on the proposed solution to Bank resources / Nominated resources (5 Resources).
- Security capability documents, as mentioned in para 6.6

The successful bidder must implement the solution within 12 weeks of releasing the Contract Order.

Sr No	Milestone	Timeline
1.	Delivery of licenses	4 weeks
2.	Submission of HLD & LLD	
3.	Implementation and Customization	6 weeks
4.	Training, UAT Sign off , Go Live & delivery of SOPs etc	2 weeks

10. Cost of bidding

The Bidder shall bear all the costs associated with the preparation and submission of its bid and the Bank will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

11. Language of bid

The language of the bid response and any communication with the Bank must be written in English only. Supporting documents provided with the RFP response can be in another language so long as it is accompanied by an attested translation in English, in which case, for purpose of evaluation of the bids, the English translation will govern.

12. Services and Adherence to Standards

a. The Bidder should ensure that the quality of delivery, adhere to quality standards/ timelines stipulated therefor.
b. The Bidder shall be willing to transfer skills to relevant personnel of NaBFID, by means of training and documentation.
c. The selected bidder should adhere to all the applicable laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities. During the course of assignment the selected bidder should provide professional and impartial suggestive measures and advices keeping the Bank's interest as paramount and should observe the highest standard of ethics while executing the agreement.

13. Clarification and Amendments on RFP / Pre-Bid Meeting:

A bidder requiring any clarification on RFP may notify NaBFID in writing strictly as per the format given in **Annexure K** by email within the date / time mentioned in the Schedule of Events. The queries received (without identifying source of query) and response of NaBFID thereof, will be conveyed to the Bidders via email or any other medium as may be deemed fit by NaBFID. NaBFID reserves the right to amend, rescind or reissue RFP, at any time prior to the deadline for submission of Bids. NaBFID, for any reason, whether, on its own initiative or in response to a clarification requested by a prospective Bidder, may modify the RFP, by amendment which will be made available to the Bidders by way of corrigendum / addendum. The interested parties / Bidders are advised to check NaBFID's email / website/GeM portal and ensure that clarifications / amendments issued by NaBFID, if any, have been taken into consideration before submitting the Bid. Such amendments / clarifications, if any, issued by NaBFID will be binding on the participating Bidders.

NaBFID will not take any responsibility for any such omissions by the Bidder. NaBFID, at its own discretion, may extend the deadline for submission of Bids in order to allow prospective Bidders a reasonable time to prepare the Bid, for taking the amendment into account. Nothing in this RFP or any addenda / corrigenda or clarifications issued in connection thereto is intended to relieve Bidders from forming their own opinions and conclusions in respect of the matters addressed in this RFP or any addenda / corrigenda or clarifications issued in connection thereto.

Any change in legal terms and conditions will be mutually agreed to only with the successful bidder. No request for change in legal terms and conditions, other than what has been mentioned in this RFP or any addenda / corrigenda or clarifications issued in connection thereto, will be entertained and queries in this regard, therefore, will not be entertained before award of the contract. Queries received after the scheduled date and time will not be responded to/acted upon.

14. Contents of Bid Document

The Bidder must thoroughly study / analyze and properly understand the contents of this RFP, its meaning and impact of the information contained therein. Misrepresentation by the Bidder or failure to furnish all information required in this RFP or submission of Bid not responsive to this RFP in any respect will be at the Bidder's risk and responsibility and the same may finally result in rejection of its Bid. NaBFID has made considerable effort to ensure that accurate information is contained in this RFP and is supplied solely as guidelines for Bidders.

The Bid prepared by the Bidder, as well as all correspondences and documents relating to the Bid exchanged by the Bidder and NaBFID and supporting documents and printed literature shall be submitted in English.

The information provided by the Bidders in response to this RFP will become the property of NaBFID and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

15. BID Preparation & Submission

Documents related to the bidding are to be submitted through GeM portal only. In case NaBFID extends the scheduled date of submission of Bid document, the Bids shall be submitted by the time and date rescheduled. All rights and obligations of NaBFID and Bidders will remain the same.

Any Bid received after the deadline for submission of Bids prescribed will be rejected.

16. Period of Bid Validity

Bid shall remain valid for a duration of 90 calendar days from Bid submission date or as may be extended. In exceptional circumstances, NaBFID may solicit the Bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A Bidder is free to refuse or not respond to the request. However, any extension of validity of Bids will not entitle the Bidder to revise / modify the Bid document.

17. Bid Integrity

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the Contract without prejudice to other actions that NaBFID may take. All the submissions, including any accompanying documents, will become property of NaBFID. The Bidders shall be deemed to license, and grant all rights to NaBFID, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

18. Bid Security/ EMD (Refundable)

The bidder should deposit bid security of Rs.3,00,000/- (Rupees Three Lac Only) in the form of a demand draft favoring National Bank for Financing Infrastructure & Development (NaBFID), payable at Mumbai or a Bank Guarantee issued from a Scheduled Commercial Bank. Bank Guarantee should be valid for a minimum of 6 months (180 days) from the date of submission of bids with a claim period of 45 days.

In case of bidders registered with NSIC/Udyog Aadhaar as MSME or a Start-up Company, they are eligible for waiver of EMD. However, SME bidders need to provide valid NSIC/MSME Certificate clearly mentioning that they are registered with NSIC under single point registration scheme or Udyog Aadhaar. Start-up bidders are required to submit Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce & Industry, Government of India. In addition, SME bidders must submit Annexure

H in physical form (Hard copy) duly signed by Chartered Accountant before the last date and time of submission of bid.

Other terms & conditions relating to Bid security is as under:

- No interest will be payable on the Bid Security amount.
- Unsuccessful Bidders' Bid security will be returned after completion of tender process. Unsuccessful Bidders should submit the Letter for Refund of EMD/Bid Security for returning of the bid security amount as per Annexure J.
- Bid Security will be forfeited in the following cases:
  - If a bidder withdraws its bid during the period of bid validity; or
  - If a Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract.
  - In case of successful bidder, if the bidder fails:
    - To execute Contract & NDA within the stipulated time or
- The successful Bidders Bid security will be discharged upon the Bidder signing the Contract Agreement & NDA.

19. Amendment of Bidding Documents

Prior to the last date for bid-submission, Bank may, for any reason, whether at its own initiative or in response to clarification(s) sought from the prospective Bidders, modify the RFP contents/ covenants by amendment. Clarification /amendment, if any, will be notified on GeM portal/ Bank's website. No individual communication would be made in this respect. In order to provide, Bidders, reasonable time to take the amendment into account for preparing their bid, the Bank may, at its discretion, extend the last date of submission of bids.

20. Authorization to Bid

The proposal/ bid being submitted would be binding on the Bidder. As such, it is necessary that authorized personnel of the firm or organization sign the bid documents. The designated personnel should be authorized by a senior official of the organization having authority. **All pages of the bid shall be initiated by the person or persons signing the bid. Bid form shall be signed in full & official seal affixed.** Any inter-lineation, erasure or overwriting shall be valid only if they are initialed by the person or persons signing the Bid. All such initials shall be supported by a rubber stamp impression of the Bidder's firm.

The proposal must be accompanied with an undertaking letter duly signed by the designated personnel providing a bid commitment. The letter should also indicate the complete name and designation of the designated personnel.
The Technical bid should contain the proof for the eligibility criteria, technical solution and un-priced Technical bid and should contain all information asked for in these documents.

In the first stage, EMD/security deposit and Integrity Pact (IP) signed by authorized signatory submitted by bidder **(Hard copies to be submitted at the Bank premise, before the expiry of bid submission date & time)** will be reviewed and if these are as per prescribed format/RFP document then only TECHNICAL BID will be evaluated. Bidders satisfying the technical requirements as determined by the Bank and accepting the terms and conditions of this document only shall be short-listed for empanelment.

21. Technical & Commercial bids

The Technical Bid should be complete in all respects and contain all information asked for in this document. The following documents are required to be uploaded to the GeM portal **(AS A**

SINGLE /COMBINED DOCUMENT ,IN THE ORDER OF PRECEDENCE) at the time of bid submission. **No other documents to be submitted/no other order of documents to be followed.**

- Annexure A - Bid form
- Annexure B - Eligibility criteria confirmation
- Company Registration proof
- Evidence for Turnover & Net worth compliance [Certificate issued by Auditor, covering Turn Over & NW for the prescribed years in tabular format]
- Evidence for support Centre at Mumbai [Office address with contact number]
- Evidence for mandatory experience [only relevant parts of the document]
- Annexure B1- Declaration of not blacklisted
- Annexure B2- Bidder details
- Annexure C1- Technical scoring sheet [Self assessed]
- Evidence to prove technical scoring for items/criteria 1 to 7
- Annexure C2- Commercial Bid **[Signed blank format to be incorporated in Technical bid and properly filled Commercials to be uploaded as Commercial Bid in GeM]**
- Annexure D-Integrity Pact
- Annexure E – Declaration of Compliance.
- Annexure F – Restrictions on procurement due to National Security.
- Annexure G – Bid security declaration.
- Annexure H – Certificate of waiver of MSE Firms, if applicable
- OEM Authorization [MAF]
- Annexure I- Functional & Technical Compliance sheet
- Copy of the RFP **[All Pages]** & its Corrigendum (if any), duly signed & sealed.

Bidders shall use Annexure J (Letter of refund of EMD) to seek back the submitted EMD post completion of the RFP process & Annexure K for Prebid queries. Further, selected bidder shall use Appendix I & Appendix II for the Non-Disclosure Agreement & Performance Bank guarantee submissions [No changes in the format is allowed later].

Non submission of the above documents at the time of bid submission will be liable for rejection of bid. Bidders are expected to examine all terms and instructions included in the documents. Failure to provide all requested information will be at the bidder's own risk and may result in the rejection of the bid.

The Bid should be signed by the authorized signatory of the bidder. A power of attorney to that effect shall be submitted by the bidders along with technical bid. Copies of relevant documents / certificates as proof in support of various information submitted in aforesaid annexures and other claims made by the bidder.

Note : Signed Integrity Pact [Annexure D] [in Rs 500 stamp paper] along with the EMD / EMD exemption declaration shall be submitted at the Bank in physical form , before the last date & time of bid submission, by all the participating bidders, in the absence of which proposals submitted in GeM portal will not be considered.

The Bank would like to expressly state that any assumption, presumptions, modifications, terms, conditions, deviation etc., which the bidder includes in any part of the Bidder's response to this RFP, will not be considered either for the purpose of evaluation or at a later stage, unless such assumptions, presumptions, modifications, terms, conditions deviations etc., have been accepted

by the Bank and communicated to the bidder in writing. The Bidder at a later date cannot make any plea of having specified any assumption, terms, conditions, deviation etc. in the Bidder's response to this RFP document. No offer can be modified or withdrawn by a Bidder after submission of Bid(s).
All the Annexures should be submitted in the prescribed format, in the letter head of bidder duly signed with seal of the company. The bidder should ensure that all the Annexures are submitted as prescribed by the Bank. In case it is not in the prescribed format, it is liable to be rejected.

In the first stage, the Bids will be opened and evaluated. Proposals of such Bidders satisfying eligibility criteria and agreeing to comply with all the terms and conditions specified in the RFP will be evaluated for technical criteria/specifications/eligibility. Only those Bids complying with technical criteria shall become eligible for further RFP evaluation process.

22. Rejection of Bid

The Bid is liable to be rejected if:

- The document does not bear the signature of authorized person in each page and duly stamped.
- It is received after expiry of the due date and time stipulated for Bid submission.
- Incomplete bids, including non-submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP) are liable for rejection by the Bank.
- It is evasive or contains incorrect information.
- Any form of canvassing / lobbying /influence/ query regarding short listing, status etc. will be a disqualification.
- Bidder should comply with all the points mentioned in the scope of work, technical specifications and all other clauses of RFP. Non-compliance of any point will lead to rejection of the bid.
- Non-submission of bid security/EMD/Integrity Pact (IP) before the last date & time of bid submission at the Bank.

23. RFP Clarifications / Bidder's queries

Queries/ clarifications will not be entertained over the phone. All queries and clarifications must to this bid be sought by email **rfp@nabfid.org** with subject "RFP FOR SUPPLY, INSTALLATION & MAINTENANCE OF CLOUD BASED VULNERABILITY MANAGEMENT SOLUTION" as per **Annexure K**

24. Technical Bid Evaluation

During the period of evaluation, bidders may be asked to provide more details and explanations about information provided in the proposals. Bidders should respond to such requests seeking explanation through GeM portal within the provided time and if the bidder does not comply or respond by the date, their bid will be liable to be rejected. It is the responsibility of bidder to check the portal in order to ascertain any clarifications are sought by bank post last date of bid submission. No separate intimation will be made by the bank to the participated bidders. If any part of the technical specification offered by the bidder is different from the specifications sought in our RFP, the bidder has to substantiate the same in detail the reason of their quoting a different specification than what is sought for, like higher version or non-availability of the specifications quoted by us, invariably to process the technical offer and it should be compatible to our application.

Setting of evaluation criteria for selection purposes shall be entirely at the discretion of the Bank. The decision of the bank in this regard shall be final and no correspondence shall be entertained in this regard.
The Bank may, at its discretion, waive any minor informality, nonconformity, or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder. Wherever necessary, observations on such minor issues (as mentioned above) Bank may be conveyed to the bidder, asking them to respond by a specified date also mentioning therein that, if the bidder does not respond by the specified date, their bid will be liable to be rejected.

25. Evaluation Methodology

a. Technical Bids received within the prescribed date and time will be opened in the presence of the authorized representatives of the firms/Company bidding who choose to attend the opening of the offer on the date and time specified in this RFP document. The Authorized representative of the firm present for the opening should have photo identification and shall sign in the register of attendance. The representative must submit an authority letter duly signed by the Firm, authorizing him to represent and attend the bid opening on behalf of the firm.

b. **For qualifying technically, the m**inimum **score will be** 60 out of total marks of 100 and the bidders who do not score 60% shall be liable to be rejected. In case during technical evaluation, all the bidders fail to score more than 60% marks, or less than three bidders obtain more than 60% marks, then at Bank's discretion, the minimum scoring criteria will be reduced to 50%. The decision of the Bank in this regard shall be final. However, Bank reserves the right to modify these criteria as per the availability of bids subsequent to the result of technical evaluation.

c. After qualifying the eligibility criteria, the bidder will be determined as a successful bidder based on QCBS (Quality and Cost Based Selection) method. In this method, the Bidder will be evaluated based on their Technical Criteria (as mentioned in Appendix-C) & Commercial Price Bid (as per Appendix- F) jointly.

d. Weightage for **t**echnical Bid & Commercial Bid will be in the ratio of **60**:**40**. The Bidders gets the highest marks cumulatively in Technical & Commercial Bid will be declared as successful Bidder. For commercial bid evaluation, the total quoted price for the VM solution product costing i.e. (1T),Container Security Module costing i.e. (2T) for a period of three (3) years and the resources cost for three (3) years i.e. (3T) shall be taken into account.

Formula for QCBS scoring:
S = (T/T-High x 60) + (C-Low/C x 40)
Where:
S = Score of the Bidder
T = Technical score of the Bidder
T-High = Highest Technical score among the Bidders
C = Quote as provided by the Firm(Total of 1T, 2T and 3T i.e. GT)
C-Low = Lowest Quote of C among the Firms
The Bidder securing the highest score becomes the successful Bidder

26. Awarding of contracts / Projects

The bidder selection will be based on Techno Commercial evaluation with a ratio of weightage of 60 (Technical score) : 40 (Commercial offer) through GeM portal. Such successful bidders shall submit Bank Guarantee for a value of 5% of the project cost (TCO) with a claim period of 3 months post completion of the project period as per the format mentioned in Appendix II.

Onboarded resource (if any) shall work from Bank premises (from its Mumbai Office) during Bank working days (Monday to Friday) from 9.30 AM to 6.30 PM , unless the Bank agrees otherwise in the respective Work Order / purchase Order of a particular project.

27. Penalties & Payment Terms

Selected bidder shall be liable to pay liquidated damages of 1% of the PO value, per week or part thereof for delay and not adhering to the time schedules of such Purchase Orders. In addition, if the project/activity includes resources to be onboarded at Bank premises, unauthorized absence of such resources during the project period /days shall attract penalty. The penalty calculation for resources is given below in the "SLA – VAPT Resources Availability" table. Resources are supposed to be working from Bank premises (unless the Bank specifies in the work order), during Bank working days & working hours.

If the selected bidder fails to complete the due performance in accordance with the terms and conditions of such Purchase Orders, the Bank reserves the right either to cancel the Purchase Order or to accept performance already made by the selected bidder. Penalty is not applicable for reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the Vendor to prove that the delay is attributable to the Bank and Force Majeure. The Vendor shall submit the proof authenticated by the Applicant and Bank's official that the delay is attributed to the Bank and / or Force Majeure along with the bills requesting payment.

Penalties for the shortfall in Performance Levels (SLAs)

a. SLA – Cloud Based Solution Availability

The Bidder shall guarantee a minimum availability (A) of 99.5% on a 24x7x365 basis for the Cloud-based solution.

Availability shall be measured on a monthly basis during the entire contract period. For the purpose of penalty calculation, the reference value shall be the yearly license/subscription cost of the VM solution.

Any shortfall in the stipulated availability shall attract penalties as defined below. The penalty shall be levied for each month in which the availability falls below the prescribed SLA threshold.

Availability percentage	Penalty Details
A >= 99.5%	No Penalty
99.5% > A >=99.0%	1% of yearly license cost of Vulnerability Management Tool
99.0% > A >= 98.5%	2% of yearly license cost of Vulnerability Management Tool

A < 98.5%	Base penalty of 2% of the yearly license cost of the VM solution, plus an additional 1% of the yearly license cost of the VM solution for every further 0.1% reduction in availability below 98.5%

b. SLA – VAPT Resources Availability

Resource SLA	Requirement	Penalty
Permanent Resource Availability during Bank working days in a month	Minimum 95% availability of the assigned resources during Bank working days in a month	A deduction of 3% from the applicable monthly service charges shall be applied for each day that the absence of resources exceeds 5%.
Replacement of Resources (if found unsuitable by the Bank for the assignment)	Replacement to be provided within 3 weeks	1 % penalty on yearly cost of resources for every week of delay thereafter
Initiation of Scheduled Scan Activities	All scan activities shall be initiated within 5 business days as per the frequency defined in the RFP and the Bank's approved activity calendar.	1% penalty on the yearly cost of the respective activity for each instance of delay.

Payment Terms
Following payment terms will be followed during the project implementation/ period

For VM and container solution:

<table>
<tr><th>SL No</th><th>Payment Milestone</th><th>Payment
[% of Project Cost]
[2T of Commercial bid doc]</th></tr>
<tr><td>1.</td><td>Delivery of licenses of all components</td><td>60 % (Payment schedule below)<table><tr><td>(at Start of) Year 1</td><td>(at Start of) Year 2</td><td>(at Start of) Year 3</td></tr><tr><td>20%</td><td>20%</td><td>20%</td></tr></table></td></tr>
<tr><td>3.</td><td>Production sign off</td><td>35%</td></tr>
<tr><td>4.</td><td>Submission of 5% BG</td><td>5%</td></tr>
</table>

For FM resources

SL No	Payment Milestone	Payment [% of Yearly Cost] *[3T of Commercial bid doc]*

1.	FM resource charges	25% per quarter (Quarterly in arrears)
2.	Annual Support / AMC / ATS for VM and container security Solution, if any	Yearly, in advance

Note: Quarterly payments shall be calculated based on the number of working days of the Bank in the respective quarter. Any non-availability of the FM resource on a Bank working day shall result in a proportionate deduction from the quarterly payment.

Payments will be made Online in INR within 30 days from Invoice submission date.

28. Right to Audit

The selected Bidder / proposed OEM infrastructure shall be subject to audit by internal / external auditors appointed by NaBFID / inspecting official from the Reserve Bank of India or peer banks or any regulatory authority, covering the risk parameters finalized by NaBFID / such auditors in the areas of services etc. provided to NaBFID and Service Provider is required to submit such certification by such auditors to NaBFID. NaBFID can make its expert assessment on the efficiency and effectiveness of security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the auditors, furnish all relevant information, records / data to them. Except for the audit done by Reserve Bank of India or any statutory / regulatory authority, NaBFID shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

Where any deficiency has been observed during audit of the Service Provider/ OEM on the risk parameters finalized by NaBFID or in the certification submitted by the auditors, the Service Provider shall correct / resolve the same at the earliest and / or within timelines stipulated by NaBFID and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the Service Provider shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed. The remediation of deficiencies will have to be done to the satisfaction of Auditors and / or NaBFID and decision of NaBFID in this regard will be final. Failure to correct / resolve any deficiencies shall entitle NaBFID to exercise any remedies available to it under this RFP / Contract including the right to terminate the Contract.

Service Provider further agrees that whenever required by NaBFID, it will furnish all relevant information, records / data to such auditors and / or inspecting officials of the NaBFID / Reserve Bank of India and / or any regulatory authority(ies). NaBFID reserves the right to call for and / or retain any relevant information / audit reports on financial and security review with their findings undertaken by the Service Provider. However, Service Provider shall not be obligated to provide records / data not related to Services under the Agreement (e.g., internal cost breakup, etc.).

29. Sub-Contracting

As per the scope of this RFP, sub-contracting is not permitted.

30. Limitation of Liability

The maximum aggregate liability of the Service Provider in respect of any claims, losses, costs, or damages arising out of or in connection with this RFP / Contract shall not exceed the Total Project Cost. Under no circumstances shall either party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

The limitations set forth herein shall not apply with respect to claims that are the subject of indemnification pursuant to infringement of third-party intellectual property rights / Damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider / Damage(s) occasioned by Service Provider for breach of confidentiality obligations / Regulatory or statutory fines imposed by a government or regulatory agency for non-compliance of statutory or regulatory guidelines applicable to NaBFID, provided such guidelines were brought to the notice of Service Provider.

31. Confidentiality

Confidentiality obligation of selected bidder shall be as per Non-disclosure Agreement placed as Appendix-I to this RFP. NaBFID reserves its right to recall all NaBFID's materials including confidential information, if stored in Service Provider system or environment, at any time during the term of the Contract or immediately upon expiry or termination of Contract. Service Provider shall ensure complete removal of such material or data from its system or environment (including backup media) to the satisfaction of NaBFID.

32. Delay in Service Provider's Performance

If at any time during performance of the Contract, Service Provider encounters conditions impeding timely delivery of the Services, Service Provider shall promptly notify NaBFID in writing of the fact of the delay, its likely duration and cause(s). As soon as practicable after receipt of Service Provider's notice, NaBFID shall evaluate the situation and may, at its discretion, extend Service Providers' time for performance, in which case, the extension shall be ratified by the parties by amendment of the Contract. Any delay in performing the obligation / defect in performance by Service Provider may result in imposition of penalty, liquidated damages and / or termination of Contract (as laid down elsewhere in this RFP document).

33. Service Provider's Obligation

Service Provider is responsible for and obliged to conduct all contracted activities in accordance with the Contract using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the Contract. It will also ensure that any change in its constitution, ownership or any material incident having a bearing on its performance obligation towards NaBFID will be immediately brought to the notice of NaBFID along with an action plan to cure deficiencies, if any, arising therefrom.
Service Provider is obliged to work closely with NaBFID's staff, act within its own authority and abide by directives issued by NaBFID from time to time and complete implementation activities.
Service Provider will abide by the job safety measures prevalent in India and will free NaBFID from all demands or responsibilities arising from accidents or loss of life, the cause of which is Service Provider's negligence. Service Provider will pay all indemnities arising from such incidents and will not hold NaBFID responsible or obligated. Service Provider is responsible for activities of its personnel and will hold itself responsible for any misdemeanors.

Service Provider shall treat as confidential all data and information about NaBFID, obtained in the process of executing its responsibilities, in strict confidence and will not reveal such

information to any other party without prior written approval of NaBFID as explained under 'Non-Disclosure Agreement' in Appendix-I of this RFP.

Without NaBFID's prior written permission, Service Provider shall not store or share NaBFID's materials including confidential information outside the geographical boundary of India or in / with a public cloud.

Service Provider agrees that it shall communicate to NaBFID well in advance along with detail plan of action, if any, changes in Service Provider's environment / infrastructure is of the nature that may have direct or indirect impact on the Services provided under the Contract or operations of its Services. Service Provider shall ensure confidentiality, integrity, and availability of NaBFID's information at all times.

34. Liquidated Damages

If the Service Provider fails to deliver and / or perform any or all the Services within the stipulated time schedule as specified in this RFP / Contract / Purchase orders, NaBFID may, without prejudice to its other remedies under the RFP / Contract, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 1 % of total Project Cost for delay of each week or part thereof. The maximum amount that may be levied by way of liquidated damages shall not exceed 10% of the Total Project Cost. Once the maximum deduction is reached, NaBFID may consider termination of the Agreement. Liquidated damages will be levied in addition to the other penalty clauses.

35. Termination for Default

NaBFID may, without prejudice to any other remedy for breach of Contract, written notice of not less than 30 (thirty) days, terminate the Contract in whole or in part:

- If the Service Provider fails to deliver any or all the obligations within the time period specified in the RFP/Contract /subsequent projects/activities during the empanelment period, or any extension thereof granted by NaBFID.
- If the Service Provider fails to perform any other obligation(s) under the RFP / Contract.
- Violations of any terms and conditions stipulated in the RFP / subsequent activity/project bid documents.
- On happening of any termination event mentioned in the RFP / Contract.

In the event NaBFID terminates the Contract in whole or in part for the breaches attributable to Service Provider, NaBFID may procure, upon such terms and in such manner as it deems appropriate, software and Services similar to those undelivered, and subject to limitation of liability clause of this RFP Service Provider shall be liable to NaBFID for any increase in cost for such similar Solution and / or Services. However, the Service Provider shall continue performance of the Contract to the extent not terminated.

If the Contract is terminated under any termination clause, Service Provider shall handover all documents / executable / NaBFID's data or any other relevant information to NaBFID in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another service provider or to NaBFID.

During the transition, the Service Provider shall also support NaBFID on technical queries / support on process implementation or in case of software provision for future upgrades.

NaBFID's right to terminate the Contract will be in addition to the penalties / liquidated damages and other actions as specified in this RFP.

36. Force Majeure

Notwithstanding the provisions of terms and conditions contained in this RFP, neither party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure. For the purposes of this clause, 'Force Majeure' means extraordinary events or circumstances beyond human control such as an act of God (like a natural calamity) or events such as wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

If a Force Majeure situation arises, Service Provider shall promptly notify NaBFID in writing of such condition and the cause thereof. Unless otherwise directed by NaBFID in writing, Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

If the Force Majeure situation continues beyond continuous period of 30 (thirty) days, either party shall have the right to terminate the Contract by giving a notice to the other party. Neither party shall have any penal liability to the other in respect of the termination of the Contract as a result of an event of Force Majeure. However, the Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of the Contract.

Termination for Insolvency:
NaBFID may, at any time, terminate the Contract by giving written notice to Service Provider, if Service Provider becomes bankrupt or insolvent or any application for bankruptcy, insolvency or winding up has been filed against it by any person. In this event, termination will be without compensation to Service Provider, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to NaBFID.

Termination for Convenience:
NaBFID, by written notice of not less than 90 (Ninety) days, may terminate the Contract, in whole or in part, for its convenience, provided same shall not be invoked by NaBFID before completion of half of the total Contract period.
In the event of termination of the Contract for NaBFID's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

37. Disputes / Arbitration (Applicable only in case of successful bidders)

All disputes or differences whatsoever arising between the parties out of or in connection with the Contract (including dispute concerning interpretation) or in discharge of any obligation arising out of the Contract (whether during the progress of work or after completion of such work and whether before or after the termination of the Contract, abandonment or breach of the Contract), shall be settled amicably. If however, the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any party notifying the other regarding the disputes, either party (NABFID or Service Provider), give written notice to other party clearly setting out therein specific dispute(s) and / or difference(s) and shall be referred to a sole arbitrator mutually agreed upon, and the award

made in pursuance thereof shall be binding on the parties. In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and arbitration proceeding shall be conducted in accordance with Arbitration and Conciliation Act 1996 and any amendment thereto. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

Service Provider shall continue to work under the Contract during the arbitration proceedings unless otherwise directed by NaBFID or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.

Arbitration proceeding shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

Applicable Law:
The Contract shall be interpreted in accordance with the laws of the Union of India and shall be subjected to the exclusive jurisdiction of courts at Mumbai.

Taxes and Duties:
Service Provider shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the commercial price bid by Service Provider shall include all such taxes in the quoted price.
All expenses, stamp duty and other charges / expenses in connection with the execution of the Contract as a result of this RFP process shall be borne by Service Provider. The Contract would be stamped as per Maharashtra Stamp Act, 1958 and any amendment thereto.

Tax Deduction at Source:
Wherever the laws and regulations require deduction of such taxes at the source of payment, NaBFID shall effect such deductions from the payment due to Service Provider. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by NaBFID as per the laws and regulations for the time being in force. Nothing in the Contract shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Contract

No Waiver of Bank Rights or Successful Bidder's Liability:
Neither any sign-off, nor any payment by the Bank for acceptance of the whole or any part of the work, nor any extension of time, nor any possession taken by the Bank shall affect or prejudice the rights of Bank against the finally selected Bidder(s), or relieve the finally selected Bidder(s) of his obligations for the due performance of the contract, or be interpreted as approval of the work done, or create liability in the Bank to pay for alterations/ amendments/ variations, or discharge the liability of the successful Bidder(s) for the payment of damages whether due, ascertained, or certified or not or any sum against the payment of which he is bound to indemnify the Bank nor shall any such certificate nor the acceptance by him of any such amount paid on account or otherwise affect or prejudice the rights of the successful Bidder against Bank.

38. RFP Ownership

The RFP, proposals by bidders and all supporting documentation are the sole property of NaBFID and should NOT be redistributed without prior written consent of Bank. Violation of

this would be a breach of trust and may, inter-alia cause the bidders to be irrevocably disqualified. The aforementioned material must be returned to NaBFID when submitting the proposal, or upon request; however, bidders can retain one copy for reference.

39. Tender/RFP Cancellation

The Bank reserves the right to cancel the Tender/RFP at any time without assigning any reasons whatsoever.

XXX

Annexure A

BID FORM (TECHNICAL BID)
[On Company's letter head]

Date: _____

To:
Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503
G block,BKC,Bandra , Mumbai - 51

Dear Sir,
Ref: RFP No.NaBFID / IS / RFP /10 dated March 30 ,2026

We have examined the above RFP, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications / modifications / revisions, if any, furnished by NaBFID and we offer to provide our consultancy services as detailed in this RFP. We shall abide by the terms and conditions spelt out in the RFP. We shall participate and submit the details as mentioned in the RFP.

While submitting this Bid, we certify that:
The undersigned is authorized to sign on behalf of the Bidder and the necessary support document delegating this authority is enclosed to this letter. We declare that we are not in contravention of conflict-of-interest obligation mentioned in this RFP. We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.

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

We undertake that we will not resort to canvassing with any official of NaBFID, connected directly or indirectly with the bidding process to derive any undue advantage. We also understand that any violation in this regard, will result in disqualification of Bidder from further bidding process.

It is further certified that the contents of our Bid are factually correct. We have not sought any deviation from the terms and conditions of the RFP. We also accept that in the event of any information / data / particulars proving to be incorrect, NaBFID will have right to disqualify us from the RFP without prejudice to any other rights available to NaBFID.

We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments / clarifications provided by NaBFID.
We agree to abide by all the RFP terms and conditions, and the guidelines quoted therein for the orders awarded by NaBFID up to the period prescribed in the RFP, which shall remain binding upon us.

In case of declaration as successful Service Provider on completion of the bidding process, we undertake to complete the formalities as specified in this RFP. Till execution of a formal contract, the RFP, along with NaBFID's notification of award by way of issuance of purchase order and our acceptance thereof, would be binding contractual obligation on NaBFID and us.
We understand that you are not bound to accept any bid you may receive, and you may reject all or any bid without assigning any reason or giving any explanation whatsoever.

We hereby certify that our name does not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity. We hereby certify that on the date of submission of bid for this RFP, we do not have any past / present litigation which adversely affect our participation in this RFP or we are not under any debarment / blacklist period for breach of contract / fraud / corrupt practices by any Scheduled Commercial Bank / Public Sector Undertaking / State or Central Government or their agencies / departments.

We hereby certify that on the date of submission of bid, we do not have any service level agreement (SLA) pending to be signed with NaBFID for more than 6 months from the date of issue of purchase order.

We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020 regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we are not from such a country or if from a country, have been registered with competent authority. We certify that we fulfil all the requirements in this regard and are eligible to participate in this RFP.

If our Bid is accepted, we undertake to enter and execute at our cost, when called upon by NaBFID to do so, a contract / service level agreement (SLA) / Memorandum of Understanding (MOU) in the prescribed form and we shall be solely responsible for the due performance of the Contract. Accordingly, we undertake that (a) we shall not withdraw or modify our bid during the period of bid validity; (b) we have not made any statement or enclosed any form which may turn out to be false / incorrect at any time prior to signing of contract; (c) if we are awarded the Contract, we shall accept Purchase Order and / or sign the Contract with NaBFID, within the specified time period in the RFP.

We further, hereby undertake and agree to abide by all the terms and conditions stipulated by NaBFID in the RFP document.

Dated this ..... day of 2026

_____

(Signature) (Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

_____Seal of the company.

Annexure B

Bidder's eligibility criteria

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents. If the Bid is not accompanied by all the required documents supporting Eligibility Criteria, the same would be rejected:

Sr. No.	Eligibility Criteria	Compliance (Yes/No)	Documents to be submitted with this tender
1.	The bidder should be registered Company / Partnership Firm / LLP under the Indian companies Act 2013 or Partnership Act 1932 or Indian LLP Act 2008 and should have office in Mumbai. The bidder should be in existence for a period of at least 5 years as on March 01, 2026.		Company's Registration document and valid address proof / relevant document for Mumbai office.
2.	The bidder should have an average annual turnover of not less than Rs.1.5 Crore in the last three FYs (i.e. 2022-23, 2023-24 & 2024-25). *Note- It should be individual company turnover and not that of any group of companies.*		Auditor's Certificate by mentioning the Annual turnover for the mentioned financial years in tabular format should be submitted.
3.	The bidder should have positive Net worth during last three financial years (i.e. 2022-23, 2023-24 & 2024-25).		Auditor's Certificate, mentioning the Net worth for the mentioned financial years in tabular format, should be submitted.
4.	The Bidder should have an experience of at least two cloud-based Vulnerability Management (VM) tool deployment, out of which one should be in BFSI sector in supply, implementation & maintenance of Cloud Based **VM tool** in India during the last 5 years.		Submit Documentary Proof (relevant parts) of Purchase Order / Work Order / sign off / any other relevant document to establish the proof.
5.	The bidder must be an OEM Authorized Seller and Service Partner for the proposed solution. Both the OEM and the bidder must have an established office presence and support infrastructure within India.		Certificate of OEM Authorized Seller and Service Partner. Office address with relevant details in company letter head to be submitted.
6.	The bidder should have minimum 5 years (as on March 01,2026) of experience in Vulnerability Management/Penetration Testing Services etc. in BFSI sector in at least 3 organizations.		Relevant supporting documents like "Award of Contract"/ "Certificate of Satisfactory Service".
7.	The cloud-based Vulnerability Management (VM) tool proposed by the bidder (OEM solution) must be deployed and operational in at least one (1) public sector or private sector banks in India with minimum 500 licenses.		PO or/and Confirmation or implementation certificate/email from the respective banks, or client reference letters on official letterhead confirming successful deployment.
8.	The bidder must be CERT-In empaneled as on the date of submission of the bid.		Copy of valid CERT-In empanelment certificate.

9.	The proposed cloud-based Vulnerability Management tool must be hosted in India. All customer data, including scan results, configuration data, and reports, must reside within India and must not be transferred outside India at any stage.		OEM self-declaration confirming data residency and hosting within India.
10.	The OEM should have more than 7 years (as on March 01,2026) in the product category of the proposed solution.		Early product commercial release date certificate by OEM.
11.	The Bidder should have at least 25 professionals having valid certification of CISSP / CISA /CISM/CCSP/OSCP /OSCE/ ISO 27001 LA /CCNP/ CEH/ CCNA as full-time employees and experience of at least THREE years in Information Security & Cyber Security domains.		Submit the declaration in company letter head
12.	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs / FIs)		Submit an Undertaking in company letterhead in this regard

Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions, in the documents submitted in pursuance of Eligibility Criteria, should be highlighted.

Name & Signature of authorized signatory
Seal of Company

Annexure B1

Declaration of Not Blacklisted

Undertaking to be submitted by all Bidders on their letter head)

Place:

Date:

To:
Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503, G block
BKC, Bandra , Mumbai - 51

We _____ (bidder name), hereby undertake that we have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response.

We also undertake that; we were never involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide / continue the services to bank.

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Company)

Date:

Annexure B2

Bidder Details

S. No.	Particulars	Details
1.	Name	
2.	Date of Incorporation and/or commencement of business	
3.	Certificate of incorporation	
4.	Brief description of the Bidder including details of its main line of business	
5.	Cert-In certification details (Copy of current & valid certificate to be enclosed)	
6.	Company website URL	
7.	Company Pan Number	
8.	Company GSTIN Number	
9.	Particulars of the Authorized Signatory of the Bidder Name Designation Address Phone Number (Landline) Mobile Number Email Address	
10	Particulars of the SPOC of the Bidder for the project Name Designation Mobile Number Email Address	

Name & Signature of authorized signatory

Seal of Company

Annexure C1

Technical Scoring sheet

Sr No	Technical Scoring Criteria	Maximum Score	Minimum Qualifying Score	Self-evaluation score	Details
1	Average Annual Turnover of the bidder in the last three financial years (i.e., 2021-22,2022-23 & 2023-24) • *>50 Crore: 10 Marks* • *>10 < = 50 Crore Turnover: 7 marks* • *= >1.5 < = 10 Crore Turnover: 5 marks*	10	5		
2	No. of Years of experience of the bidder in IT infrastructure/ Information Security/ Cyber Security related activities in India in BFSI Sector. *(Evidence of the 1st assignment to be enclosed as proof of experience /experience will be counted from the date of most relevant evidence)* • *>10 Years: 15 Marks* • *>7 to <=10 Years: 10 marks* • *> = 5 to <=7 Years: 5 marks*	15	5		
3	No of desirable points complied by the proposed solution in Technical & Functional requirements of this RFP and the marks will be awarded as follows: • *All points: 15 marks* • *More then 80 Pct compliance :10 Marks* • *Less then 80 Pct compliance: 5 marks* • *Less than 50 Pct compliance : 0 marks*	15	5		
4	Skilled Employees / Resources on bidder's payroll with any of the certificates like OSCP/OSWE/ eWPTX / API Security Certified Practitioner / Offensive Mobile Security Expert / eMAPT/ CEH, CHFI • More than 15: 10 Marks • 5 to 14 Employees: 7 Marks • Less than 5 Employees :0 Marks *(Declaration on official letter head signed by competent authority to be submitted*	10	7		

	along with copy of certificates)				
5	Number of Cloud Based VM solution projects carried out by the bidder for BFSI in India during last five financial years from the date of this RFP. Five marks per assignment for different activities/projects *(Purchase Order/Work Order/ sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence)*	15	5		
6	Number of implementations of the proposed Cloud Based VM solution (proposed OEM specific) in BFSI/ Central Govt/ Regulated Entities in India during last five financial years from the date of this RFP. Five marks per assignment for different activities/projects *(Purchase Order/Work Order/ sign off/ work completion confirmation or any other relevant document by OEM agreed by the Bank to be submitted as evidence)*	15	5		
7	The bidders shall be required to make a detailed technical presentation and demonstration before the Bank's Evaluation Committee. The presentation shall carry 20 marks out of 100 technical marks and shall be evaluated based on the following criteria: (i) understanding of the Bank's requirements and regulatory expectations (ii) technical architecture and solution design (iii) functional demonstration aligned to RFP requirements (iv) security and compliance features (v) competency of proposed resources and (vi) implementation and support approach.	20	10		
Total Marks		100			

Note: The bidder must obtain a minimum of 60 out of 100 marks overall and meet the minimum qualifying marks specified for each individual point in technical scoring sheet, failing which the bid shall be disqualified.

Annexure C2

Commercial Bid format
Implementation, Management & Maintenance of Cloud Based Vulnerability Management (VM) Solution

[Cost in INR]

Sr	Item	Cost per year per license/asset A	Cost per year B =A *500	Taxes, if any C	No of years D	Total Cost E= (B+C)*D
1	**Vulnerability Management Product Costing**					
1a	License cost for Cloud Based Vulnerability Management Solution for 500 assets *[#500 licenses]*				3	
1b	One-Time Implementation & Deployment Cost				NA	
1T	TOTAL				NA	
2	**Container Security Module Costing [From Same OEM]**					
2a	License cost for container scanning solution from same OEM [6 Worker nodes or master nodes] (If additional cost is involved)				3	
2b	One-Time Implementation & Deployment Cost				NA	
2T	Total				NA	
3	**Resources Costing**					
3a	Yearly Costing – one L1 resource for VA & Container vulnerability Scanning (Images & running containers) configuration Scans(As per SCDs) as per the scope and frequency mentioned in Section 7.	NA			3	
3b	Yearly Costing-For Network PT, Application PT, Mobile PT and API security Testing as per the scope and frequency mentioned in Section 7.	NA			3	

3d	Annual Support / AMC / ATS for VM and container security Solution, if any				3	
3T	Total				NA	
GT	**Grand Total (1T +2 T+3T)**				**NA**	
4	**Product cost for Year 4 & Year 5 [Optional Item]** *(Mandatorily to be quoted)*					
4a	Cost for year 4 & 5 [includes license cost, support cost & other costs, if any]				2	
4b	Cost for year 4 & 5 – one L1 resource for VA & compliance Scans as per the scope and frequency mentioned in Section 7.	NA			2	
4c	Cost for year 4 & 5 -For Network PT, Application PT, Mobile PT and API security Testing as per the scope and frequency mentioned in Section 7.	NA			2	
4d	Cost for year 4 & 5 License cost for container scanning solution from same OEM [5 Worker nodes or master nodes]					
4e	Yearly Costing- For Container vulnerability Scanning (Images & running containers) & configuration checks (As per SCDs) for nodes using VM tool procured through this bid as per the scope and frequency mentioned in Section 7.					
5	**Product cost discovery for later expansion**					
5a	License cost for a bundle of 100 VM licenses**				NA	
5b	License cost for a bundle of 6 worker/master node licenses for container scanning **				NA	

** *Quoted price will be applicable for years 1 to 5*

Additional Rate Card for Ad-hoc Security Scanning Requirements:

S.No.	Scanning Type	Assets/Application Scope	Total Cost
1	Network Penetration Testing (PT)	5 IPs	
2	Application PT as per latest OWASP top 10 & SANS Top 25	5 Applications	
3	API security testing as per latest OWASP top 10 & SANS Top 25	5 API	
4	***Source Code review as per latest OWASP ASVS, OWASP Top 10, SANS Top 25, and NIST SP 800-218 (SSDF) using bidder tools.	2 Applications	
5	Mobile application security testing (SAST & DAST) as per latest OWASP MASVS, OWASP Top 10, SANS Top 25, and NIST SP 800-163.	1 Application	
6	Container vulnerability Scanning (Images & running containers) & configuration checks for nodes using standard tools	2 Worker nodes or master nodes	

****Bank may require to perform Source Code review on Adhoc basis.*

Note :

1. ***The bid evaluation shall be based on the Grand Total (1T + 2T + 3T), and the bidder shall enter the same value in the GeM portal while submitting the commercial bid.***
2. *If disparity in quote between figures & words, commercial quote written in words will be considered as final.*
3. *Payments will be released against submission of original invoices & sign off by the Bank.*
4. *The offered commercials shall have a validity of 90 days from the date of the offer.*
5. *Commercial offer shall be in the letter head of the company, with office seal.*
6. *The Bank is currently seeking price discovery from bidder for conducting source code review using standard tools brought by the bidder and may ask vendor to perform the same at a later stage, as per requirement during the contract period.*
7. *Required hardware components at locations where Bank's applications are hosted will be provisioned by the Bank. All the hardware requirements at OEM location/Data Centre should be included in the commercials quoted.*

(Signature)

Name & Designation of the authorized signatory:

Company Name:

Date:

Annexure D

Integrity Pact

Tender Ref.No: NaBFID/IS/ RFP/10 dated March 30 ,2026

INTEGRITY PACT

(To be Stamped as an Agreement)

Between

NATIONAL BANK FOR FINANCING INFRASTRUCTURE AND DEVELOPMENT, a statutory body established under the National Bank for Financing Infrastructure and Development Act, 2021 having its office at the Capital, A Wing, 15th Floor- 1503, G Block, Bandra Kurla Complex, Bandra (East), Mumbai – 40005, hereinafter referred to as "The Principal,"

and

_____ hereinafter referred to as "The Bidder/ Contractor."

Preamble

The Principal intends to award contract/s for_____, under laid down organisational procedures, The Principal values full compliance with all relevant laws of the land, rules, regulations, economical use of resources, and fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

To achieve these goals, the Principal shall appoint Independent External Monitors (IEMs) who shall monitor the tender process and the execution of the contract for compliance with the abovementioned principles.

Section 1 – Commitments of the Principal

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

a. No employee of the Principal, personally or through family members, shall in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

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

c. The Principal shall exclude from the process all known persons having conflict of interest.

Section 2 – Commitments of the Bidder(s)/ Contractor(s)

1) The Bidder(s)/ Contractor(s) commits themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractor(s) commits themselves to observe the following principles during participation in the tender process and the contract execution.

a. The Bidder(s)/ Contractor(s) shall not, directly or through any other person or firm, offer, promise, or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which they are not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or the execution of the contract.

b. The Bidder(s)/ Contractor(s) shall not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal, in violation of the Competition Act, 2002 (as amended from time to time). This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the tender process.

c. The Bidder(s)/ Contractor(s) shall not commit any offence under the relevant IPC/PC Act; further, the Bidder(s)/ Contractor(s) shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals, and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details, as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers," shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines, all the payments made to the Indian agent/representative must be in Indian Rupees only.

e. The Bidder(s)/ Contractor(s) shall, when presenting their bid, disclose any and all payments made, is committed to, or intends to make to agents, brokers, or any other intermediaries in connection with the award of the contract.

f. Bidder(s) /Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision.

g. If the Bidder/Contractor or any employee of the Bidder/Contractor or any person acting on behalf of the Bidder/Contractor, either directly or indirectly, is a relative of any of the officers of the Employer, or alternatively, if any relative of an officer of the Employer has financial interest/stake in the Bidder(s)/Contractor(s) firm (excluding Public Ltd. Company listed on Stock Exchange), the same shall be disclosed by the Bidder/Contractor at the time of filling of tender. The term 'relative' for this purpose would be as defined in Section 2(77) of the Companies Act 2013.

2) The Bidder(s)/ Contractor(s) shall not instigate third persons to commit offences outlined above or be an accessory to such offences.

3) The Bidder(s)/Contractor(s) shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the Employer.

Section 3 - Disqualification from the tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution, has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per laid down procedure to debar the Bidder(s)/Contractor(s) from participating in the future procurement processes of the Government of India.

Section 4 – Compensation for Damages

1) If the Principal has disqualified the Bidder(s) from the tender process before the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

2) If the Bidder makes an incorrect statement on this subject, the Principal shall act like para 2) of Section 4 above.

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

In the case of Sub-contracting, the Principal Contractor shall take responsibility for adopting the Integrity Pact by the Sub-contractor.

a. The Principal shall enter into agreements with identical conditions as this one with all Bidders and Contractors.

b. The Principal shall disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of the conduct of a Bidder, Contractor, or Subcontractor, or of an employee or a representative or an allied firm of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal shall inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor

1) The Principal shall appoint competent and credible Independent External Monitor(s) for this Pact

after approval by the Central Vigilance Commission. The task of the Monitor is to review, independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2) The Monitor is not subject to instructions by the parties' representatives and performs their functions neutrally and independently. The Monitor would have access to all Contract documents whenever required. It shall be obligatory for them to treat the information and documents of the Bidders/Contractors as confidential. They report to the Management of the Principal.

3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction, all Project documentation of the Principal, including that provided by the Contractor. Upon their request and demonstration of a valid interest, the Contractor shall also grant the Monitor unrestricted and unconditional access to their project documentation. The same applies to Subcontractors.

4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and 'Absence of Conflict of Interest.' In case of any conflict of interest arising later, the IEM shall inform the Management of the Principal and recuse themselves from that case.

5) The Principal shall provide the Monitor with sufficient information about all meetings among the parties related to the Project, provided such meetings could impact the contractual relations between the Principal and the Contractor. The parties offer the Monitor the option to participate in such meetings.

6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, they shall inform the Management of the Principal and request the Management to discontinue or take corrective action or other relevant action. The Monitor can, in this regard, submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action, or tolerate action.

7) The Monitor shall submit a written report to the Management of the Principal, within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

8) If the Monitor has reported to the Management of the Principal a substantiated suspicion of an offence under the relevant IPC/ PC Act, and the Management of the Principal has not, within the reasonable time, taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9) The word 'Monitor' would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders, 6 months after the contract has been awarded. Any violation of the same would entail disqualifying the bidders and exclusion from future business dealings.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this Pact as specified above, unless it is discharged / determined by the Management of the Principal.

Section 10 – Other provisions

1) This agreement is subject to Indian Law. The place of performance and jurisdiction is the place from where the Tender/ Contract is issued.

2) Changes, supplements, and termination notices must be submitted in writing. Side agreements have not been made.

3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties shall strive to come to an agreement according to their original intentions.

5) Issues like Warranty / Guarantee, etc., shall be outside the purview of IEMs.

---------Sd----------	----------Sd----------
(For & On behalf of the Principal)	(For and on behalf of Bidder/ Contractor)
(Office Seal)	(Office Seal)

Place ---------- Date ----------

Witness 1: _____ Witness 1: _____
(Name & Address) (Name & Address)

Annexure E

Declaration for Compliance
(In Company letterhead)

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

Signature:
Name
Date
Seal of company:

Technical Specification

We certify that the systems/services offered by us for tender confirm the specifications stipulated by you with the following deviations

List of deviations

1) _____

2) _____

3) _____

4) _____

Signature:

Name
Date
Seal of company:

(If left blank it will be construed that there is no deviation from the specifications given above)

Annexure F

Restriction on Procurement due to National Security

(This Certificate should be submitted on the letterhead of the bidder)

Date:

To,

Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503, G block
BKC, Bandra, Mumbai - 51

Ref.: RFP No.: _____ Dated: _____

I have read the clause regarding restrictions on procurement from a bidder/OEM of a country which shares a land border with India; / certify that this bidder is not from such a country or, if from such a country, have been registered with the Competent Authority. I hereby certify that this bidder fulfills all requirements in this regard and is eligible to be considered. (Where applicable, evidence of valid registration by the Competent Authority shall be attached.)

I have read the clause regarding restrictions on procurement from a bidder/OEM of a country which shares a land border with India and on subcontracting to contractors from such countries; I certify that this bidder is not from such a country or, if from such a country, have been registered with the Competent Authority and will not subcontract any work to a contractor from such countries unless such contractor is registered with competent authority. I hereby certify that this bidder fulfills all requirement in this regard and is eligible to be considered. (Where applicable, evidence of valid registration by competent authority shall be attached)

Yours faithfully,

Authorized Signatory
Name:
Designation:
Vendor's Corporate Name
Address

Email and Phone :

Annexure G

Bid Security Declaration

To,
Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503, G block
BKC,Bandra , Mumbai - 51

Dear Sir,

Subject: Request for Proposal (RFP) for the supply, implementation & maintenance of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution in NaBFID

We _____ (bidder name), hereby undertake that we are liable to be suspended from participation in any future tenders of the Bank for 2 years from the date of submission of Bid in case of any of the following:

If the bid submitted by us is withdrawn/modified during the period of bid validity.
If any statement or any form enclosed by us as part of this Bid turns out to be false / incorrect at any time during the period of prior to signing of Contract.

In case of we becoming successful bidder and if we fail to execute Contract within the stipulated time/ we fail to furnish Performance Bank Guarantee within the timelines stipulated in this RFP document.

Yours faithfully,

Date: For _____

Signature _____

Name _____

Annexure H

Certificate of Waiver for MSE Firms

(in Letter head of Chartered Accountant)

Date:
TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s. _____, having registered office at _____has made an original investment of Rs._____/- in _____, as per Audited Balance Sheet as on ……. Further we certify that the Company is classified under Micro and Small Enterprise (MSE) as per MSME Act 2006 and subsequent government notifications.

We have checked the books of the accounts of the company and certify that the above information is true and correct.

Chartered Accountant Firm Name

Signature
Name
Reg.No

Firm
Seal

VID No.

Annexure I

Functional and Technical Compliance Sheet

There are certain requirements that are mandatory in nature, the remaining parameters are desirable as indicated below. Bids shall be rejected for non-compliance to below mandatory points.

I. General Requirements

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	The solution must be a cloud-based SaaS platform hosted in India.	Mandatory	
2.	Solution must support multi-user RBAC with SSO/SAML and MFA.	Mandatory	

II. Asset Discovery and Inventory Management

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	Automatic discovery of known and unknown assets across on-prem, cloud, containers, and endpoints	Mandatory	
2.	Give the user the flexibility to create dynamic tags basis on "asset name", "asset inventory", IP address and range, open ports, vulnerability, etc.	Desirable	
3.	Must identify and tag software to either Commercial or Opensource software	Desirable	
4.	Ability to view asset, software, ports, certificates, and vulnerabilities on a unified dashboard.	Desirable	
5.	Ability to scan IPs simultaneously and the rest of the IP's /asset scheduled for scanning (in any site) to be able to put in the scanning queue and run automatically.	Mandatory	
6.	The solution must support advanced query and search features for assets and vulnerabilities, including: • Elastic search-like query capability with filtering and sorting. • Ability to save and reuse queries for recurring analysis and reporting.	Desirable	
7.	The solution must provide a customizable and interactive dashboard that allows users to:	Desirable	

	• Create and personalize dashboards based on asset search queries. • Convert clicks or filters into query-based views. • Drag and drop widgets for repositioning and layout customization. • Apply color coding to represent risk levels or categories (e.g., high, medium, low).		
8.	The dashboard must offer rich visualization and drill-down capabilities, including: • Multiple widget formats (pie charts, bar charts, value indicators, and list views). • Drill-down from summary views to detailed asset and vulnerability data. • Daily trend visualization within widgets for tracking changes over time. •Should be able to convert a query into a widget	**Desirable**	

III. Vulnerability Management

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	Support for authenticated and unauthenticated scans for OS, databases, applications, and network & security devices.	Mandatory	
2.	Should support authentication support but not limited to Linux, Windows, Network and Security devices (Checkpoint FW, Cisco, Cisco APIC Infoblox, Network SSH, Palo Alto FW, SNMP), Applications (Apache, BIND, Docker, HTTP, Jboss, MS IIS, Kubernetes, NGINX, Tomcat, Oracle Weblogic etc.), Databases (Azure MS SQL, Cassandra, IBM DB2, MariaDB, MongoDB, MS SQL, MySQL, Oracle, SAP HANA, PostgreSQL etc.), VMware for authentication	Mandatory8.	
3.	Should support integration with authentication vaults - CyberArk PIM,	Mandatory	

	CyberArk AIM, Thycotic, Beyond trust PBPS, Hashicorp, Azure Key, Arcon PAM, Liebeman ERPM, Wallix (WAB).		
4.	Enables discovery of assets in the environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets.	Mandatory	
5.	Gather detailed information, such as an asset's details, running services, installed software, and more and eliminate the variations in product and vendor names and categorize them by product families on all assets.	Desirable	
6.	Must include CVE-to-detection mapping and CVSSv2/v3.	Mandatory	
7.	The solution must leverage global threat intelligence frameworks such as MITRE ATT&CK to map vulnerabilities with corresponding tactics and techniques, thereby enabling threat-informed vulnerability prioritization and remediation planning.	Desirable	
8.	The solution must enrich vulnerabilities with real-time threat indicators (RTIs) sourced from both internal and external feeds (e.g., CISA KEV, public exploits, malware associations, zero-day alerts, and active exploitation data). It should automatically tag vulnerabilities with contextual attributes such as *Actively Exploited, Easy Exploit, High Data Loss, Denial of Service, No Patch, Exploit Kit,* etc., to support risk-based remediation and improve visibility into real-world exploitation trends.	Desirable	
9.	Allow risk scoring based on exploitability, business impact, and lateral movement potential.	Desirable	
	Should have an automated way to "Ignore" vulnerabilities with easy tracking for exception management and/or false positives	Mandatory	

10.	Support Static and Dynamic tagging for asset management, scanning and reporting	Desirable	
11.	Should support out of box query/token for assets and vulnerabilities like threat hunting any asset with vulnerability having remote code execution or ransomware associated to it	Desirable	
12.	Integration with ITSM tools (e.g., ServiceNow) ,GRC archer and SIEM solutions through API.	Desirable	
13.	Should support unlimited multiple sensors for inventory - virtual scanners, agents, container sensors etc for asset inventory.	Desirable	
14.	Option to group the assets basis on OS, software, tags, last logged in user, created, last seen etc.	Desirable	
15.	The solution must support agent-based, agentless, and hybrid scanning modes. Able to scan a host (wherever applicable) with agent and scanner both consuming only single license	Mandatory	
16.	Must encrypt scan data in transit and at rest.	Mandatory	
17.	Support custom and predefined reports (Executive, Technical, PCI, etc.) in PDF/CSV formats.	Mandatory	
18.	Able to provide remediation suggestion in the scan reports	Mandatory	
19.	The solution must be capable of tracking the status of each vulnerability across iterative scans, including its lifecycle state (e.g., new, existing, or reopened) to ensure accurate remediation tracking and trend analysis. It should also display key timeline details such as the initial date of discovery, last observed date, and closure verification date (where applicable).	Mandatory	
20.	Auto updating & self managing scanners and agents	Mandatory	
21.	Should have the ability to auto-eliminate superseding patches	Mandatory	

22.	Should provide information if the vulnerability has a virtual patch available	Desirable	
23.	Report generation through API	Desirable	
24.	Have the capability for Automatic correlation between CVE and Patch KB	Mandatory	
25.	Option to group the vulnerabilities basis on name, age, severity, cvss rating, vendor, vendor product name, OS, status, malware name, RTIs, Public exploit, exploit kit etc.	Desirable	
26.	Schedule discovery/map scans and vulnerability scans and sent the notification before and after scan completion.	Mandatory	
27.	The quoted license cost for the Vulnerability Management Solution shall be based on number of assets, where an asset shall be defined as a unique host or endpoint identified by a unique IP address, hostname, or agent installed on the system. The following shall be considered a single asset: • Server (Physical or Virtual) • Desktop / Endpoint • Network Device (Firewall, Router, Switch, Load Balancer) • Cloud Instance / VM Multiple services, open ports, applications, or domains running on the same host shall not be counted as separate assets. The solution must support agent-based and agentless scanning within the same license without additional cost.	Mandatory	
28.	The proposed Vulnerability Management Solution shall support unlimited vulnerability scans of assets for which licences are taken during the contract period.	Mandatory	

	The license shall not restrict: • Number of scans • Number of scan schedules • Number of vulnerability signatures/plugins • Number of scanning policies • Number of scanning engines required within the licensed asset limit. The Bank may perform on-demand, scheduled, or continuous scanning without additional licensing cost.		
29.	The proposed solution must support vulnerability scanning for on-premise and cloud environments including workloads hosted in public cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform without additional licensing cost within the asset limits.	Mandatory	

V. Agent Security

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	Agent should provide a continuous view of assets for vulnerability management, configuration assessment, and asset inventory without the need for credential management, and firewall changes required by network scanner deployments.	Mandatory	
2.	Agent's design should focus on "One Agent - Multiple Capabilities" which means same agent shall be performing inventory, vulnerability, configuration assessment, asset management (including security use cases), Software Composition Analysis (SwCA), Passive Sensing etc.	Desirable	
3.	Solution should be able to merge the scan data from agent and scanner and	Mandatory	

	provide a single instance for the vulnerability		
4.	The agent shall be lightweight with a low CPU and memory footprint, designed for high-performance functionality. It should capture only delta changes in metadata and securely transmit them to the management server for centralized processing, analysis, reporting, and configuration management.	Mandatory	
5.	Agent should be light weight, have a low CPU and memory footprint which shall bring the high-performance functionality of the agent & built in configurations for central management	Desirable	
6.	Users shall be able to uninstall the agents which are not reporting to the management server automatically or manually from the UI	Mandatory	
7.	Agent should be self updating and tamper resistant	Mandatory	
8.	Lightweight, auto-updating agent supporting Agent-based detection (On prem) Agent Support Windows (client and server versions) Agent Support Linux and Unix Agent Support Mac OS Agent Support AIX Agent Support for ZLinux Agent Support for Solaris Agent Support for Gentoo Agent Support for ChromeOS	Mandatory	

VI. Container Security

The bidder shall indicate any additional licensing requirements for the container security module, if applicable, which may be procured separately by the Bank based on necessity. The proposed module shall be from same OEM.

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	The proposed solution should be from same OEM and capable of scanning container workloads (with additional licenses if required) and integrate with the Vulnerability Management solution for unified reporting and dashboarding.	Mandatory	
2.	The solution must provide end-to-end container security, including runtime protection, image scanning, and continuous vulnerability management for containers, images, and registries without requiring manual intervention.	Desirable	
3.	The solution shall support clustered container orchestration environments like Kubernetes, OpenShift, Docker Swarm and managed services like AKS, ECS, EKS, OKE etc.	Mandatory	
4.	Ability to scan directly into Red Hat Enterprise Linux CoreOS in Red Hat OpenShift, to identify vulnerabilities and manage risk at both RHCOS OS and container levels.	Mandatory	
5.	Should support container security with scanning for images, registries (ECR, GCR, JFrog, etc.), and runtime workloads.	Mandatory	
6.	The solution shall have the ability to do automatic discovery, Inventory of all the containers and images with all metadata.	Mandatory	
7.	Support for Software Composition Analysis (SCA) and malware/secret detection in container images	Desirable	
8.	The solution must have detailed vulnerability information like identification, analysis, CVSS score, remediation etc. for containers.	Mandatory	
9.	The solution shall perform configuration and compliance checks on running containers, provide remediation for failed checks, and support exception management for approved deviations. It must support management of vulnerability, compliance, access, and	Desirable	

	audit controls in containerized environments.		

V. Support and SLA

Sr No	Solution Capabilities	Mandatory/Desirable	Compliant (Yes/No)
1.	OEM / Bidder must provide 24x7 support through email and portal.	Mandatory	
2.	Critical issue response time: ≤ 12 hours; Medium: ≤ 48 hours; Low: ≤ 3 business days.	Mandatory	
3.	Availability of a Technical Account Manager (TAM) during the contract period from OEM.	Desirable	

Annexure J

LETTER FOR REFUND OF EMD

(To be submitted by the unsuccessful bidders, post completion of the procurement process)

Date:
To,
Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503, G block
BKC,Bandra , Mumbai - 51

We _____ (Company Name) had participated in the Request for Proposal (RFP) the supply, implementation & maintenance of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution in NaBFID and we are an unsuccessful bidder.

Kindly refund the EMD submitted for participation. Details of EMD submitted are as follows

Sr. No.	Bidder Name	DD/BG Number	Drawn on (Bank Name	Amount (Rs)

Bank details to which the money needs to be credited via NEFT are as follows

1. Name of the Bank with Branch
2. Account Type
3. Account Title
4. Account Number
5. IFSC Code

Sign

Name of the signatory

Designation

Company Seal.

Annexure K

Pre-Bid Query Format
(To be provided strictly in Excel format)

Vendor Name	Sl. No	RFP Page No	RFP Clause No.	Existing Clause	Query/Suggestions

APPENDIX I

NON-DISCLOSURE AGREEMENT FORMAT
[To be submitted by the successful bidder]

This Non-Disclosure Agreement (hereinafter referred to as the "**Agreement**") is made and executed on this [*date*] day of [*month*]**,** [*year*]**.**

BY AND BETWEEN

National Bank for Financing Infrastructure and Development, An All India Financial Institution established under the National Bank for Financing Infrastructure and Development Act, 2021, having its office at The Capital, A Wing, 15th Floor- 1503, G Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400051, (which expression, unless repugnant to the context or meaning thereof, shall mean and include its successors and permitted assigns) of the First Part.

AND

[●], a company incorporated and registered under the provisions of Companies Act, 1956/2013, having its registered office at_____, (which expression, unless repugnant to the context or meaning thereof, shall mean and include its successors and permitted assigns) of the other Part.

For the purposes of this Agreement, **NaBFID** and _____may be collectively referred to as the "**Parties**" and individually as the "**Party**"

"Disclosing Party" means the party disclosing / sharing Confidential Information to the other party.

"Receiving Party" means the party receiving Confidential Information from the Disclosing Party.

WHEREAS,

A. The Parties hereto are in the process of _____("**Purpose**") and plan to engage in mutual discussions connected thereto.

B. It may be necessary for a Party to disclose to the other, information pertaining to, but not limited, to its business, customers, intellectual property, which is proprietary and confidential of either Party and/or its subsidiaries (defined hereunder and referred to as "confidential information"); and

C. The Parties desire to protect the confidentiality of any confidential information disclosed or exchanged pursuant hereto.

NOW, THEREFORE, in consideration of the promises and covenants herein set forth and for other good and valuable consideration, the receipt, adequacy, and legal sufficiency of which are hereby acknowledged, the Parties mutually agree as follows

1. Definitions

1.1 Unless otherwise the context requires, the following terms as used in this Agreement shall have the respective meanings as defined below:

1.1.1. **"Confidential Information"** means any part and all tangible or written expression of information and data of a commercial or technical nature, which relates to or concerns the business, operations and assets of the Disclosing Party or the Purpose which includes but is not limited to trade and technical secrets, any information which the Disclosing Party has rights to as the owner thereof whether at common law or by statute; financial information, internal operating procedures, customer related information, investment strategies, statistics, data, know-how research, photographs, notes, renderings, journals, notebooks, computer programs, source codes, object codes, audio files, sound files, plans, products, services, personal and confidential records of patients, personally identifiable information/data, personal health information/data & record inventions, developments, patents, intellectual property, designs, drawings, hardware and software configuration information.

Provided Confidential Information does not include information which:

a) is required by law, statute or any judicial, quasi- judicial, governmental or other regulatory authority to be disclosed, provided, the Disclosing Party is given a prompt notice of such requirement, wherever possible, to enable it to defend itself from such disclosure and Receiving Party shall ensure that the scope of such disclosure is limited to the extent possible; or

b) is or becomes part of the public domain otherwise than as a result of any default or breach of confidentiality on the part of the Receiving Party; or

c) is known to the Receiving Party prior to the disclosure by the Disclosing Party without an obligation to keep such Confidential Information confidential; or

d) is subsequently obtained by the Receiving Party from a third party without breach of any obligation of confidentiality owed to any third party or the Disclosing Party; or

e) is independently developed by the Receiving Party or a person within the Receiving Party without any breach of this Agreement as evidenced by written records; or

f) was in the Receiving Party's legal possession before receipt from the Disclosing Party.

If the Receiving Party seeks the benefit of any of the aforesaid exceptions, it shall bear the burden of proving its existence.

1.1.2. **"Effective Date"** shall mean the date agreed to between the Parties for commencement of the Agreement and on which this Agreement becomes effective. In the absence of any written agreement to this effect, the date of execution of this Agreement shall be deemed to be the Effective Date.

2. Confidentiality Obligations

2.1. Receiving Party agrees that, it shall:

2.1.1. maintain all Confidential Information in strict confidence in accordance with the provisions hereof and shall not disclose, or cause or permit the disclosure of any Confidential Information except as permitted under this Agreement or with the prior written consent of the Disclosing Party;

2.1.2. not distribute or disclose any Confidential Information, in any way or form, to anyone except to any personnel/employee/representative of the Receiving Party or any third-party recipient, each of whom:

a. reasonably needs to know such Confidential Information for the Purpose; and

b. is bound to legally enforceable confidentiality obligations in writing towards the Receiving Party, that are not less stringent than the obligations imposed on the Receiving Party under this Agreement.

2.1.3. implement and maintain reasonable safeguards with respect to the handling and management of all Confidential Information (with the same degree of care as is used in relation to the Receiving Party's own equally important confidential information) so as to ensure the confidentiality and secrecy thereof;

2.1.4. not copy or reproduce any Confidential Information (or any part thereof) by any means whatsoever, except as may be reasonably necessary to carry out the Purpose;

2.1.5. promptly notify the Disclosing Party if it suspects or becomes aware of any unauthorized use, storage, copying or disclosure of the Confidential Information;

2.1.6. be liable for all the acts and/or omissions of its third-party recipients, personnel, employees, representatives, wherein, the disclosure of Confidential Information has resulted in unauthorized distribution, use and/or disclosure of such Confidential Information;

2.1.7. comply with all applicable data privacy and protection laws and regulations that relate to privacy laws and the privacy and security of Personally Identifiable Information and Personal Health Information etc;

2.1.8. not be construed as granting or conferring any rights (including but not limited to, intellectual property rights) by license or otherwise, expressly, impliedly or otherwise, in respect of any of the Confidential Information disclosed by the Disclosing Party;

2.1.9. not unlawfully profit or take unfair advantage of any Confidential Information disclosed to it or enable, procure or assist others (including any of its agents, consultants, servants or employees) to do so;

2.1.10. act in good faith and always be bound by the confidentiality obligations of this Agreement and for so long as the information disclosed to it by the Disclosing Party is or remains as Confidential Information within the meaning of this Agreement.

2.1.11. adhere to all applicable data protection laws and guidelines.

2.1.12. implement appropriate security measures to protect data against unauthorized access, breaches, or misuse.

2.1.13. This clause shall survive in perpetuity.

3. Representations and Warranties

3.1. Each Party represents and warrants to the other that:

3.1.1. it has the authority to enter into this Agreement and to do all things necessary for the performance of this Agreement;

3.1.2. the information is made available "*as-is*", and no warranties are given, or liabilities of any kind assumed, in relation to the quality of such information, including but not limited to, its fitness for the Purpose or its correctness;

3.1.3. this Agreement is not intended to constitute, create, give effect to, or otherwise recognize a joint venture, partnership or formal business entity of any kind. Any exchange of the Confidential Information under this Agreement shall not be deemed as constituting any offer, acceptance, or promise of any further contract or amendment to any contract, which may exist between the Parties. Each Party shall act as an independent contractor/party and not as an agent of the other Party for any purpose whatsoever and neither shall have any authority to bind the other;

3.1.4. neither Party nor its representatives shall use the other Party's name, in any advertising, sales or promotional material, or in any publication without the prior written consent of the other party except for internal communications to affiliates of such party (including publications);

3.1.5. this Agreement does not constitute a commitment or promise by either Party hereto to proceed with the Purpose. Until and unless definitive agreements between the Parties with respect to the Purpose have been executed and delivered, neither Party will be under any legal obligation of any kind whatsoever with respect to the Purpose by virtue of this Agreement, except for the provisions specifically agreed to herein.

4. Term and termination

4.1. This Agreement shall come into effect from [●] (**"Effective Date"**) and shall continue for a period of _____ years ("**Term**"), unless terminated earlier with thirty (30) days prior written notice by either Party.

4.2. The Recipient's obligations in relation to Confidential Information disclosed prior to expiry of this Agreement, as well as the remedies available under this Agreement, shall survive the expiry of this Agreement for the Survival Period of _____ years.

4.3. Upon expiration or termination of this Agreement, the Receiving Party shall:

4.3.1. On the request of the disclosing party, either (i) return or (ii) destroy, any documents, whole or partial copies, records, reproductions, writings and any other matters or materials as may exist in any form of media, whether in hard copy, electronic form, tangible form, storage or in any manner or form which contain any Confidential Information, without making, duplicating or retaining any copies in any form howsoever, other than for any legal or regulatory requirements.

4.4. The Parties agree that all Confidential Information disclosed by the Disclosing Party to the Receiving Party and all confidentiality obligations provided pursuant to this Agreement shall be binding on the Receiving Party during the Term of this Agreement and shall continue to be binding even after the termination or expiration of this Agreement in perpetuity.

5. Remedy for Breach

5.1. The Receiving Party hereby expressly acknowledges that any breach by the Receiving Party of its covenants, obligations and agreements of confidentiality as expressed in this Agreement may cause the Disclosing Party to suffer and/or incur serious irreparable harm and injury and/or loss where monetary damages would be inadequate to compensate the Disclosing Party for such breach by the Receiving Party. Accordingly, in the event of any breach or threatened breach by the Receiving Party of any of the provisions of this Agreement, the Disclosing Party shall, in addition to and not in limitation of any other rights, remedies, recourse or damages available to the Disclosing Party at law or in equity, the Disclosing Party shall be entitled to seek injunctive relief whether in the form of a temporary, interim or permanent restraining order or injunction or other equitable relief, against the Receiving Party to prevent or restrain any such further or continued unauthorized disclosure of its Confidential Information by the Receiving Party, or by any other person directly or indirectly acting for, on behalf of, or with the Receiving Party.

6. Governing Law and Jurisdiction

6.1. This Agreement shall be governed by the applicable laws of India and in case of any dispute arising out of or in relation to this Agreement shall be subject to the exclusive jurisdiction of the Courts situated at Mumbai

6.2. All or any unresolved disputes between the Parties with regard to the meaning, construction, and implementation of this Agreement which cannot be resolved amicably within 15 days between the Parties either by mediation or conciliation, then, the same shall be resolved by submitting such dispute/s to the Arbitration of a sole Arbitrator to be mutually nominated in writing by the Parties in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or as amended from time to time. The seat of Arbitration shall be in Mumbai and the Arbitration proceedings shall be held in English. The Parties agree that the decision of the Arbitrator shall be final and binding on the Parties.

7. Miscellaneous

7.1. **Notices**: Any notice required to be given hereunder or pursuant to law shall be sufficient if it is in writing and if and when it is hand-delivered or sent by registered mail to the address mentioned in the cause title or any other address as may be notified by the Parties.

7.2. **Entire Agreement**: This Agreement constitutes the entire agreement between the Parties and supersedes all oral negotiations, prior agreements, arrangements, and understandings of any sort whatsoever relating to the subject matter hereof (including, without limitation, fees and other compensation).

7.3. **Severability**: If any provision of this Agreement is held to be illegal, invalid, or unenforceable under any present or future law, the remaining provisions of this Agreement shall remain in full force and effect and shall not be affected by the illegal, invalid, or unenforceable provision or by its severance here from.

7.4. **Waiver**: The failure, with or without intent, of any Party to insist upon the performance by the other Party, of any term or stipulation of this Agreement, shall not be treated as or be deemed to constitute a waiver of such right of such Party.

7.5. **Modification**: No modification, amendment, or variation of this Agreement will be effective or binding on the Parties unless it is written and signed by both Parties.

7.6. **Assignment**: Neither Party shall assign or otherwise transfer any rights or duties under this Agreement to any third party without the prior written consent of the other Party.

7.7. **Counterparts**: This Agreement may be executed in two counterparts, both of which shall constitute one document, and each Party to the Agreement shall be entitled to retain one counterpart of the Agreement.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement on the day and year first written above**.**

By: _____

Name:

Designation:

National Bank for Financing Infrastructure and Development

By: _____

Name:

Designation:

[Company Name]

APPENDIX II

PERFORMANCE BANK GUARANTEE

(To be submitted by the successful bidder, post project allotment)

Note:
This guarantee should be furnished by a Nationalized Bank / Scheduled Bank, as per the following format.
This bank guarantee should be furnished on stamp paper value as per Stamp Act. (not less than Rs.500/-).

To:
Chief Information Security Officer
National Bank for Financing Infrastructure & Development (NaBFID)
The Capital, A wing, 15th floor – 1503, G block
BKC, Bandra , Mumbai - 51

Dear Sir,
In consideration of To: Chief Information Security Officer, National Bank for Financing Infrastructure & Development (NaBFID), The Capital, A wing, 15th floor – 1503, G block, BKC, Bandra , Mumbai – 51, placing an order under the procurement process for the supply, implementation & maintenance of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution project in NaBFID, _____(company name) having registered office at _____ (hereinafter called the vendor) as per the purchase contract entered into by the vendor vide purchase contract no _____ dated _____ (hereinafter called the said contract), we _____(Name of the Guarantor Bank), a 'schedule bank', issuing this guarantee through its branch at _____ presently located at _____ (hereinafter called the bank), do hereby irrevocably and unconditionally guarantee the due performance of the vendor as to the) for Request for Proposal (RFP) for the supply, implementation & maintenance of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution as per the said contract entered into by the vendor with you.
If the said vendor fails to implement or maintain the system or any part thereof as per the contract and on or before the schedule dates mentioned therein, we _____ (Name of the Guarantor Bank), do hereby unconditionally and irrevocably agree to pay the amounts due and payable under this guarantee without any demur and merely on demand in writing from you during the currency stating that the amount claimed is due by way of failure on the part of the vendor or loss or damage caused to or suffered / or would be caused to or suffered by you by reason of any breach by the said vendor of any of the terms and conditions of the said contract, in part or in full. Any such demand made on us shall be conclusive as regards the amount due and payable under this guarantee.

We _____(Name of the Guarantor Bank), further agree that this guarantee shall continue to be valid will you unless you certify that the vendor has fully performed all the terms and conditions of the said contract and accordingly discharge this guarantee, or until _____ , whichever is earlier. Unless a claim or demand is made on us in writing under this guarantee on or before _____, we shall be discharged from all our obligations under this guarantee. If you extend the schedule dates of performance under the said contract, as per the terms of the said contract, the vendor shall get the validity period of this guarantee extended suitably and we agree to extend the guarantee accordingly at the request of the vendor and at our discretion, provided such request is served on the bank on or before _____.

Failure on part of the vendor in this respect shall be treated as a breach committed by the vendor and accordingly the amount under this guarantee shall at once become payable on the date of receipt of demand made by you for payment during the validity of this guarantee or extension of the validity period.

You will have fullest liberty without affecting this guarantee to postpone for any time or from time to time any of your rights or powers against the vendor and either to enforce or forebear to enforce any or all of the terms and conditions of the said contract. We shall not be released from our liability under this

guarantee by the exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the vendor or any other forbearance act or omission on your part or any indulgence by you to the vendor or by any variation or modification of the said contract or any other act, matter or thing whatsoever which under the law relating to sureties would but for the provisions hereof have the effect of so releasing us from our liability hereunder.

In order to give full effect to the guarantee herein contained you shall be entitled to act as if we are your principal debtors in respect of all your claims against the vendor hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provision of this guarantee.

The words the vendor, the beneficiary of this guarantees i.e. Yourself, and ourselves i.e. _____(Name of the Guarantor Bank), unless repugnant to the context or otherwise shall include their assigns, successors, agents, legal representatives. This guarantee shall not be effected by any change in the constitution of any of these parties and will ensure for and be available to and enforceable by any absorbing or amalgamating or reconstituted company or concern, in the event of your undergoing any such absorption, amalgamation or reconstitution.

This guarantee shall not be revocable during its currency except with your prior consent in writing. This guarantee is non-assignable and non-transferable.

Notwithstanding anything contained herein above:
Our liability under this bank guarantee shall not exceed 5% of the project cost. This bank guarantee shall be valid up to _____. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only if you serve upon us a written claim or demand (and which should be received by us), on or before _____ 12:00 hours (Indian standard time) where after it ceases to be in effect in all respects whether or not the original bank guarantee is returned to us.

This guarantee deed must be returned to us upon expiration of the period of guarantee

Signature ……

Name ……
(In Block letters)
Designation ……
(Staff Code No.)……

Official address:
(Bank's Common Seal)
Attorney as per power of Attorney No.
Date:

WITNESS:
1…… (Signature with Name, Designation & Address)
2…… (Signature with Name, Designation & Address)