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 & MAINTENANCE OF CLOUD BASED SECURE WEB GATEWAY/ PROXY, CLOUD BASED VIRTUAL PRIVATE NETWORK (VPN)/ ZERO TRUST NETWOK ACCESS (ZTNA) & DATA LOSS PREVENTION (DLP) SOLUTION

Ref: NaBFID / IS / RFP /06 dated July 21,2025

GEM Bid Ref No:

(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
August 11, 2025, 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	Last date for requesting clarification/Queries	Up to 4.00 PM on July 26,2025 All communications regarding points / queries requiring clarifications shall be given by email to rfp@nabfid.org
4	Last date and time for Bid submission	Up to 4.00 PM on August 11,2025
5	Address for submission of Bids	Through GeM portal
6	Date and Time of opening of Technical Bids	4.30 PM on August 11,2025 *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.*
7	Announcement of shortlisted bidders	Shall be communicated subsequently
8	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.

Contents

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 the qualified bidder for the supply, implementation and maintenance of Cloud based Secure Web Gateway/ Proxy, Cloud Based Virtual Private Network (VPN)/ Zero Trust Network Access (ZTNA) and Data Loss Prevention (DLP) solution to secure the Bank's endpoint devices and network access.

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 Appendix – B on the achievement of which a Bidder becomes eligible for technical Bid.
j) "Eligibility Claim" means the claim against the criteria listed in Appendix – B submitted by the Bidder to become eligible for technical Bid.
k) "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.
l) "Scheduled Commercial Bank" means all banks are included in the second schedule to the Reserve Bank of India Act, 1934.
m) "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 technical criteria & eligibility criteria mentioned in Annexure-A & Annexure-B (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) is as given below.

Level 1 (L1)	Educational Qualifications: Graduation Experience: Minimum two years of experience in IT, out of which a minimum of one year of experience in the proposed cloud solution for secure gateway/ proxy, VPN/ ZTNA and DLP.
Level 2 (L2)	Educational Qualifications: Graduation Experience: Minimum 5 years of experience in IT, out of which minimum three years of experience in web proxy, VPN and DLP (including two years' experience in the proposed cloud solution for secure gateway/ proxy, VPN/ ZTNA and DLP.)

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 Secure Web Gateway/ Proxy, cloud-based VPN/ Zero Trust Network Access (ZTNA) and Data Loss Prevention (DLP) solution to enforce granular controls over the endpoint devices that connect to the Bank's network infrastructure. The scope includes the supply, implementation and maintenance of the Cloud based Secure Web Gateway/ Proxy, Cloud based VPN/ Zero Trust Network Access and Data Loss Prevention (DLP) solution based on the following requirements (not limited to):

General Requirements:

- The Bank intends to implement a Cloud based Secure Web Gateway solution for 500 users and Data Loss Prevention solution for 500 users/ endpoints and a cloud-based VPN/ Zero Trust Network Access solution for 200 users from day one of implementation.
- The proposed cloud-based solution for Secure Web Gateway/Proxy, VPN/ZTNA and DLP solutions must be from the same OEM.
- The proposed cloud based solution for secure web gateway, VPN/ZTNA and DLP solution should have a minimum of 4 OEM's own/ co-located data centres hosted in different seismic zones in India, all with local processing and compute.
- As part of the data localization, all the data traffic from the Bank's endpoint devices to the proposed cloud-based solution for secure web gateway, VPN/ ZTNA and DLP solution must be restricted to the OEM's own/ co-located data centres hosted in India only.
- The solution should not have any destination cloud/ backend architecture which requires routing of traffic within the solution to different data centres for traffic processing
- The proposed cloud-based solution should be capable to manage all the security controls intended through secure web gateway, VPN and DLP solution through the deployment of a single/unified agent at the endpoint device.
- The solution agent must be tampering proof and for additional security the endpoint agent must support one time password of random alphanumeric characters per device and can only be used once for logout, disable individual services, uninstall etc.

- The proposed cloud-based solution for secure web gateway, VPN and DLP solutions should support the deployment of wide range of endpoint devices like laptop, IPAD, Android devices etc.
- The solution should support various operating systems like Microsoft Windows, MAC, IOS, Android, Linux etc.
- All the proposed solution should support Zero Trust Network Access architecture by default.
- The solution must support seamless integration with the Bank's existing SIEM solutions (LogRythm & Gurucul) without any additional cost to the Bank.
- The proposed solution should support the integration with Bank's ITSM solution (Freshservice) without any additional cost to the Bank.
- The solution should support the integration of standard Threat Intel Services available in the market by means of STIX /TAXII or through APIs.
- There should not be any limitation in the blocking of IOCs including IP addresses, domains, URLs, Hash Values etc in the proposed cloud based secure web gateway, VPN/ ZTNA and DLP solutions.
- 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
- The SOC 2 Type 2 audit reports & certificates of the proposed cloud-based solutions should be shared with the Bank on annual basis.
- 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.
- 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.
- **The OEM must implement the proposed solution and provide 24x7x365 premium support with 30 minutes response time for P1 tickets with dedicated/ (or) shared TAM (Technical Account Manager)**
- The proposed solution must not have a single point of failure and should have seamless auto failover to the secondary site (running with the same capacity & specified features) if the primary site goes down.
- The proposed solution must have in-built data log retention of at least 1 year from for all components.
- The selected bidder should provide training for the selected Bank officials on the proposed solutions without any additional cost to the Bank.
- The endpoint agent must have inbuilt debugging capabilities.

6.1 Cloud Based Secure Web Gateway/ Proxy

The Bank plans to implement a cloud bases Secure Web Gateway (SWG) or proxy solution that offers robust content filtering, internet access control, malware detection, and threat prevention.

The solution must authenticate users, monitor cloud application usage, and support centralized policy management with comprehensive reporting.

- The solution shall include Web Proxy with Caching, Web Content Filtering, URL filtering, Anti Malware, Anti-Virus, Application layer filtering, Sanboxing, Layer-7, Application control features etc.
- The solution should have inbuilt set of URL filtering capabilities with pre-defined and custom categories.
- The solution should have the built-in intelligence to identify and control any website with Generative AI capabilities.
- The proposed system must identify and monitor cloud applications over a wide range of services such as Microsoft 365, AWS, Google Cloud, GitHub, Microsoft Azure cloud, ChatGPT by OpenAI, Microsoft Copilot, GitLab, Power BI, Webex, Darwinbox, BoardPAC and other cloud-based SaaS/ PaaS/ IaaS platforms.
- Cloud Access Security Broker will be a mandatory part of the proposed solution.
- The solution should support hybrid deployment without any additional cost to the Bank.
- The proposed solution should support integrations with multiple Identity Providers.
- The solution must support 500 users from day one of implementation.

6.2 VPN/ Zero Trust Network Access

The Bank intends to deploy a cloud-native private access solution that ensures secure, high-performance access to internal applications, regardless of user location. The solution must support user authentication, device posture checks (e.g., configuration, patching, antivirus status, Windows activation, Active Directory integration etc.), and offer centralized policy and reporting features.

- The cloud native private access solution must provide Zero Trust Network Access irrespective of user locations (corporate LAN, branch P2P/ MPLS, remotely).
- The solution must work on Zero Trust Principle and must be capable to identify and authenticate the end user, device, the means of access and to authorize the user access based on least privilege and need to know basis.
- The solution should have the ability to centrally define, deploy, and immediately enforce policies for all users, across all locations from a single console
- The solution must have capability to restrict the access based on Geo- locations.
- The proposed solution should support integrations with multiple Identity Providers.
- The solution should be intelligent enough with the ability to User-App-Segmentation in LAN for Office and Branch Users. Internal applications traffic should not be sent to Internet for LAN users.
- The proposed solution should have capability to apply Zero Trust locally in the DC where application is hosted.
- The license model will be purely based on user license and the solution must support 200 users from day one of implementation. The Bank will not be subject to any license-based limitations or restrictions when integrating its applications with the proposed solution. Any additional license costs associated with integrating the Bank's applications during the contract period shall be borne solely by the bidder.

6.3 Cloud Based Data Loss Prevention (DLP) Solutions

The Bank plans to implement a cloud native Data Loss Prevention (DLP) solution to monitor, detect and prevent the unauthorized transmission or exposure of sensitive data -such as Personally Identifiable Information (PII), financial records, and intellectual properties etc. (not limited to)- across cloud services, endpoints and network. The solution should cover all the aspects of both endpoint and web based DLP solutions and should offer offer centralized policy and reporting features.

- The solution must provide real-time monitoring and policy enforcement for data in use, motion and at rest across all platforms.
- The solution must be capable enough to enforce policy based on the metadata.
- The solution must integrate seamlessly with the proposed cloud based Secure web gateway/proxy, VPN/ ZTNA.
- The solution should be capable to identify the Bank's document based on its data classification.
- The DLP solution should have built-in compliance templates and pre-defined identifiers.
- The proposed solution should have advanced Optical Character Recognition (OCR), Fingerprinting etc.
- The solution must support 500 users/endpoints from day one of implementation.

Functional & Technical Requirements

I. Cloud Based Secure Web Gateway/ Proxy

Sr No	Solution Capabilities	Compliance (Yes/No)
1.	The solution must have a complete license for Web content filtering, Anti-Malware, SSL/TLS Inspection, Content Inspection, Advanced Threat Protection, Application Visibility and Control, Bandwidth Control, Visibility and Control of all ports and protocols, and Advanced Reporting with at least 1-year built in log retention.	
2.	The proposed solution must have the ability to handle all web and non-web traffic, across all ports and protocols, with infinite elastic scalability and unbeatable performance	
3.	The proposed solution must support policy creation based on defined criteria such as users, user groups, device trust status, geographic location, URL categories, cloud applications, destination IP addresses, custom URLs, and similar attributes.	
4.	The solution must support device posture of the endpoints prior to granting internet access as part of the proposed Zero Trust Architecture. The basic device posture checks should include a check for Microsoft Intune compliance, OS version, Host firewall status, Antivirus status etc. with provision to define custom check as well.	

	The device posture checks must be supported in Android and IOS devices too	
5.	The solution must support comprehensive full inspection of both inbound and outbound internet traffic, including all versions of SSL/TLS-encrypted communications, regardless of port or protocol.	
6.	The solution must have the ability to create custom categories based on URLs	
7.	As a deterrent control, the solution must support user warning prompts/ caution message prior to access attempts to predefined websites.	
8.	The solution should be able to identify and block SSH and IRC tunneling attempts to prevent communication with Command and Control (C2) servers	
9.	The proposed solution should support both agent bases and agentless approach without compromising in the functionalities offered.	
10.	The proposed solution should enforce session blocking for certificates that are expired, issued by unrecognized authorities, have unresolved status, or encounter timeouts during validation etc.	
11.	The proposed solution should have the capability to create custom file-type control policies based on users, groups, type of applications, action type (upload and download) etc.	
12.	The solution must be capable of detecting and blocking phishing websites.	
13.	The proposed solution should have a dynamic risk scoring mechanism to evaluate the potential risk of the URLs accessed by the end users. It should support the auto-blocking of such high risk categorized URLs.	
14.	The proposed solution must have built-in Intrusion Prevention System (IPS) functionality for all web protocols like HTTP, HTTPS etc.	
15.	The proposed solution should support at least 5 devices (Laptop/ Desktop/ Mobile/ IPAD etc.) for a single authenticated user	
16.	The solution should support bandwidth throttling for large file downloads during business hours.	
17.	For effective utilization of the available Bank's network bandwidth, the proposed solution must provide the functionality for bandwidth caping based on users/ groups/ application accessed etc.	
18.	The solution should have an inbuilt DNS security solution to ensure safe browsing for end user.	

19.	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time.	
20.	The solution must be able to support XFF (XForwarded-For) to identify the source IP address of a host for effective correlation through SIEM.	
21.	The solution must feature a real-time threat intelligence and content filtering platform that includes regularly updated signatures and blacklists for high-risk categories such as phishing, malware, pornography, extremism, gambling, anonymizing services, C2 servers, ransomware, keyloggers, fraudulent websites etc.	
22.	The proposed solution must provide comprehensive web security that can identify and block malicious scripts (e.g., JavaScript, VBScript), executable files, unauthorized ActiveX controls, potentially unwanted programs, shareware, and cross-site content access.	
23.	The solution must enforce controls to restrict file uploads and downloads based on file type extensions and should intelligently detect and block files even if their extensions are altered or renamed.	
24.	The solution must support end-to-end encryption for data in transit, utilizing the latest industry-standard security protocols.	
25.	The solution must have the capabilities to inspect malware embedded in PDF, word, PPT files, etc.	
26.	The platform must support (allow/block/inspect) QUIC protocol, DoH, DoT etc.	
27.	The proposed solution must have the option to schedule automated backups within the admin console to create backups periodically without manual intervention to ensure compliance with the organization's Business Continuity Plans and Disaster Recovery Plans.	
28.	The solution must provide Role based access control (RBAC) for different user groups based on their job role for solution management.	
29.	The SSL/TLS Inspection platform must support inspection of different types of compression algorithms including nested compressed files.	
30.	The SSL/TLS inspection performed should be on real time basis and there must not be any latency induced by the SSL/ TLS inspection which will impact the end user experience.	
Cloud Access Security Broker (CASB)		
31.	The proposed solution must have the ability to auto discover, monitor, and control access to all popular cloud applications.	

32.	The solution must support the creation of detailed access control policies for Microsoft 365 applications (e.g., OneDrive, SharePoint, Teams), Google applications (e.g., Google Drive, Gmail, Google Doc) etc. including controls over file uploads, downloads, sharing, and security inspection.	
33.	The solution must support tenant (corporate vs personal tenants) base restrictions on the cloud web/ applications access.	
34.	The solution should have granular control over all popular social web applications like Facebook, LinkedIn, X(Twitter), YouTube, Instagram and others.	
35.	The solution must have the capability to create custom policies for Bank's cloud-based applications/ Web.	
36.	The solutions must have predefined cloud app (Microsoft Teams, CISCO WebEx, ZOOM, OneDrive, SharePoint, Google Drive etc.) policies for profiling and blocking.	

II. VPN/ Zero Trust Network Access

Sr No	Solution Capabilities	Compliance (Yes/No)
37.	To strengthen overall security, the proposed solution should deliver consistent Zero Trust Network Access (ZTNA) for all users—whether they're connecting from the corporate LAN, branch offices via MPLS, or remotely—under a unified policy framework.	
38.	The proposed solution must have the ability to User-App-Segmentation in LAN for Office and Branch Users. Internal App traffic should not be sent to the Internet for LAN Users.	
39.	The solution should provide user to application segmentation and connect users to specific applications and limit lateral movement.	
40.	To eliminate the attack surfaces, the proposed solution must support application access through outbound service-initiated connections (unidirectional inside-out connections) i.e., it should not require any inbound firewall rule from OEM's cloud platform and only outbound traffic should be allowed.	
41.	The connectivity between the user's device and the private applications must be end to end encrypted and the traffic should be optimally routed to the nearest data centers to ensure low latency.	
42.	The application publishers/ connectors must operate in high availability (HA) and support built-in load balancing.	
43.	The solution must support regular re-authentication of users or per app re-authentication after a certain configurable time period.	
44.	The proposed solution should support at least 5 devices (Laptop/ Desktop/ Mobile/ IPAD etc.) for a single authenticated user	

45.	The solution should have the ability to control access based on geolocation and must be able to block all traffic coming from hostile countries.	
46.	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time.	
47.	The proposed solution should be capable of providing secure private application access to all TCP and UDP based applications.	
48.	The endpoint agent must have inbuilt debugging capabilities.	
49.	The solution must be able to support XFF (XForwarded-For) to identify the source IP address of a host for effective correlation through SIEM.	
50.	The solution should enforce policies based on the following parameters but not limited to: • User • Group • User attributes (Roles, Departments etc) • User domains (e.g. corporate vs personal)	

III. Cloud Based Data Loss Prevention Solution

Sr No	Solution Capabilities	Compliance (Yes/No)
51.	The proposed solution must have the ability to provide both Web based Data loss prevention and Endpoint level Data loss prevention.	
52.	The Solution must support the creation of DLP policies using parameters such as content, keywords, data patterns, metadata, file size, upload URLs, user groups etc. or any combination thereof.	
53.	There must not be any dependencies on the type/version of web browsers to enforce the DLP policies.	
54.	The solution must support the creation of DLP policies based on various data classification labels implemented through M365.	
55.	To enhance data protection, the solution should leverage AI and ML capabilities to analyze and understand sensitive content, including documents and images, and use sophisticated detection methods to safeguard against web-based data leaks.	
56.	The solution must block users from performing upload/downloads based on file type, document classification labels, file size etc.	
57.	The proposed solution must have predefined templates to identify PII data classifiers like, PAN, Aadhar, Card BIN, Account No , Voter ID Card No etc., IP	
58.	The proposed solution should give a prompt for user if any violation of DLP policies are flagged. Feature for capturing the justification from the end users must be incorporated in the prompt.	

59.	To prevent unauthorized data transfer, the Endpoint DLP must offer USB Device Control, enabling admins to enforce policies based on device attributes such as manufacturer, model, serial number, and device ID, and assign rules per user or group.	
60.	The solution must provide Content inspection for data movement to peripheral devices like USB, printers etc. with allow, block, User Alert actions etc.	
61.	The solution must support offline enforcement of Endpoint DLP policies, with comprehensive device control over USB, printer access, LAN connectivity, and Bluetooth communication etc.	
62.	The proposed solution must support advanced features like OCR, AI/ML, fingerprinting to safeguard organizations from various means of data leakage.	
63.	The solution must support time-bound DLP exclusions, allowing administrators to grant temporary exclusions that automatically expire after a specified duration.	
64.	The solution must enforce the DLP policies against the exclusion given for external sharing for one-drive in M365 to prevent Data loss.	
65.	The proposed solution must seamlessly restrict the sharing of sensitive data using various platforms like Microsoft email exchange, Microsoft Teams, Microsoft OneDrive, Microsoft SharePoint etc.	
Administration, Management & Reporting (Secure Web Gateway, VPN/ ZTNA, DLP)		
66.	The proposed solution must be able to integrate with Bank's on-premises Active Director (AD)	
67.	The solution must be able to integrate with SAML 2.0 (Azure AD, OKTA and ADFS etc.).	
68.	The solution must have the support for multi factor authentication for login to admin console.	
69.	To get better granular and easily readable reports, the proposed solution must provide minimum 1 year log retention period within OEM's platform for each web transaction.	
70.	For advanced analytics and forensic purposes, the proposed solution must provide at least 90 days of globally correlated real-time interactive reporting for every web transaction.	
71.	To troubleshoot critical performance related issues faster, the proposed solution must provide the proxy latency and server response time for every web transaction as part of its reporting.	
72.	The proposed solution must have the ability to do every transaction level logging (not summarized logging) with detailed information including but not limited to: Timestamp, User Agent, Source IP, Destination IP, User, Destination Port, Applications, URL, URL	

	Category, Policy Action etc.	
73.	The solution should have the ability to schedule the executive summary reports based on Bank's requirement.	
74.	The solution must provide complete audit trail logs for all the admin activities.	
75.	The solution should be capable of generating granular level custom reports such as but not limited to: 1) Usage Report of Specific User/IP/Group based on Date/Time 2) Report for all users who have accessed a specific URL 3) Usages report based on Date & Time 4) Top service user 5) Most requested service, etc.	
76.	The solution must have advanced built-in packet capture capability for troubleshooting.	
77.	The solution must provide full reporting including malware behavior and intent, indicators of compromise (IOCs), dropped files, PCAPs etc.	
78.	The proposed solution must have the ability to monitor internet-based SaaS applications as well as other custom internet-based destinations (e.g., websites, web-based apps, third party proxy etc.)	
79.	The solution should provide advanced threat dashboard to track the infection or threat history for User/IP with the ability to access all forensic evidence for past infections (at least 1 year)	
80.	The solution should be able to schedule reports and provide the flexibility to generate on demand reports in daily/weekly/monthly/yearly or specific range.	
81.	The solution should support custom report creation in Excel, pdf, etc.	
Availability (Secure Web Gateway, VPN/ ZTNA, DLP)		
82.	To guarantee uninterrupted business operations, the OEM must commit to a 99.995% availability SLA covering all in-line, non-in-line, integration, and reporting services, with no exceptions or exclusions.	
83.	The solution must provide advanced threat protection (ATP) capabilities with an uptime SLA of 99.995% for all traffic (all ports/protocols) without any third-party integrations.	
84.	The solution must commit to ensure minimum latency in processing encrypted traffic which is ideally <= (60 ms to 110 ms) on an hourly basis.	
85.	The endpoint agent in the proposed solution must support business continuity during cloud infrastructure outages by offering a disaster recovery mode. This mode should allow administrators to grant	

	access solely to pre-approved business-critical internet applications for enrolled users, avoiding traditional fail-open or fail-close behaviour.	

7. Bank's existing infrastructure

Details of the cloud ecosystem infrastructure in use in the Bank are mentioned in the below given table. Bidders shall ensure that the offered Cloud based Secure Web Gateway, VPN/ZTNA & DLP solution is compatible/capable to manage the underlying cloud infrastructure mentioned in the table.

Sr No	Cloud Deployment Model/ Services	Application Count
1	Private Cloud	14
2	SaaS	5
3	Public Cloud	2

Note: If any additional details on Bank's IT infrastructure are required by any of the prospective bidders for preparation of bidding documents, the same may be intimated over email. Bank will provide required information /response (at its discretion) one to one.

8. 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 on the proposed solution to Bank resources / Nominated resources.

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	5 weeks
4.	Training, UAT Sign off , Go Live & delivery of SOPs etc	3 weeks

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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 or Bank Guarantee 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 N 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 I.
- 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.

18. 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.

19. 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 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.

20. 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 **(ONLY 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 6
- 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 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 **[Page 1 -29]** & 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.

21. 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.

22. 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 the implementation of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution" as per **Annexure K**

23. 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.

24. 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.

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
C-Low = Lowest Quote of C among the Firms
The Bidder securing the highest score becomes the successful Bidder

25. 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.

26. 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 will be Rs. 1000/- per day of absence of L1 resource & Rs. 2500/- per day of absence of L2/L3 resources. 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)

Vendor will have to guarantee a minimum availability [A] of 99.995%, calculated on a monthly basis. Solution availability will be 99.995% on 24x7x365. The penalty will be calculated as per the details given below.

Availability percentage	Penalty Details
A >= 99.995%	No Penalty
99.995% > A >=99.99%	2% of cost of monthly charges
99.99% > A >= 99.9%	5% of cost of monthly charges
A < 99.9%	Penalty at an incremental rate of 1% (in addition to a base of 5%) of monthly charges for every 0.1% lower than the stipulated uptime

Payment Terms

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

SL No	Payment Milestone	Payment [% of Project Cost] *[1T of Commercial bid doc]*
1.	Delivery of licenses of all components	50%
2.	Submission of HLD/LLD Documents & acceptance by the Bank	10%
3.	Implementation UAT sign off	10%
4.	Production sign off	25%
5.	Submission of 5% BG	5%
Recurring Cost		
1.	Annual Charges[AMC/ATS]	Yearly, in advance
2	FM resource charges, if any	Quarterly, in arrear

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

27. 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.).

28. Sub-Contracting

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

29. 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.

30. 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.

31. 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).

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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 Union 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.

38. 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. Ref: NaBFID / IS / RFP /06 dated July 21,2025.

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 2025

_____

(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, 2025.		Company's Registration document and valid address proof / relevant document for Mumbai office.
2.	The bidder should have an annual turnover of not less than Rs.1 Crore in the last three FYs (i.e. 2021-22, 2022-23 & 2023-24). *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. 2021-22, 2022-23 & 2023-24).		Auditor's Certificate, mentioning the Net worth for the mentioned financial years in tabular format, should be submitted.
5.	The Bidder should have an experience of at least two, out of which one should be in BFSI in India in supply, implementation & maintenance of Cloud Based Secure Web Gateway and VPN/ ZTNA 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.
6.	The Bidder should have at least five professionals having valid certification of ***CISSP / CISA /CISM/CCSP/OSCP /OSCE/ ISO 27001 LA /CCNP/ CEH/ CCNA / Advanced level certification in the proposed Solution(only technical)*** as full-time employees and experience of at least THREE years in Information Security & Cyber Security domains.		Submit the declaration in company letter head
7.	Bidder and OEM should have office presence/ Support Centre in India.		Office address with relevant details in company letter head to be submitted
8.	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	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: 15 Marks* • *>10 < = 50 Crore Turnover: 10 marks* • *>1 < = 10 Crore Turnover: 5 marks*	15		
2	No. of Years of experience of the firm 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: 20 Marks* • *>7 to <=10 Years: 15 marks* • *> = 5 to <=7 Years: 10 marks*	20		
3	Number of Cloud Based Secure Web Gateway and VPN/ ZTNA carried out by the SI for BFSI/Central Govt/ Regulatory bodies/ Listed Companies in India during last five financial years from the date of this RFP. Three 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		
4	Latency in processing encrypted traffic on an hourly basis must be shared from the respective OEM and the marks will be awarded as follows: • *<= 60 ms: 5 marks* • *>60 ms to <=100 ms: 3 marks* • *>100 ms to <= 110 ms: 1 marks*	5		
5	Skilled Employees / Resources on bidder's payroll with an experience of more than 2 years related to Information Technology, Information Security & Cyber Security domains. • More than 50: 15 Marks • 26 to 50 Employees: 10 Marks • 25 or less Employees :5 Marks *(Declaration on official letter head signed by competent authority to be submitted)*	15		
6	Number of Cloud Based Secure Web Gateway and VPN/ ZTNA projects carried out by the SI for	10		

	Banks /AIFIs in India [specifically, excluding RRBs &Co-operative Banks] during last five financial years from the date of this RFP. Two 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)*			
7	Number of implementations of the proposed Cloud Based Secure Web Gateway and VPN/ ZTNA (proposed OEM specific) in BFSI/ Central Govt/ Regulatory bodies/ Listed Companies in India during last five financial years from the date of this RFP. Four 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)*	20		
Total Marks		100		

Annexure C2

Commercial Bid format
Implementation, Management & Maintenance of Cloud Based Secure Web Gateway, VPN/ ZTNA & DLP Solution

[Cost in INR]

Sr	Item	Cost per year A	Taxes, if any B	No of years C	Total Cost D= (A+B)*C
1	**Product Costing**				
1a	License cost *[500 Proxy & DLP licenses & 200 VPN licenses]*			3	
1b	One Time Implementation Cost			NA	
1c	Any other cost, involved in the deployment of the project, including support cost, if any			3	
1T	TOTAL				
2	**Facility Management Costing [Optional Item]** *(Mandatorily to be quoted)*				
2a	Yearly Costing – one L1 resource			3	
2b	Yearly Costing – one L2 resource			3	
3	**Product cost for Year 4 & Year 5 [Optional Item]** *(Mandatorily to be quoted)*				
3a	Cost for year 4 & 5 [includes license cost, support cost & other costs, if any]			2	
4	**Product cost discovery for later expansion**				
4a	License cost for a bundle of 50 web proxy & DLP licenses*			NA	
4b	License cost for a bundle of 20 VPN licenses*			NA	

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

Note :

1. *If disparity in quote between figures & words, commercial quote written in words will be considered as final.*
2. *Payments will be released against submission of original invoices & sign off by the Bank.*
3. *The offered commercials shall have a validity of 90 days from the date of the offer.*
4. *Commercial offer shall be in the letter head of the company, with office seal.*
5. *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 /06 dated July 21,2025

Whereas NaBFID constituted under the National Bank for Financing Infrastructure and Development Act, 2021 having its headquarters at Mumbai acting through its Chief Information Security Officer's(CISO) Office, represented by Chief Information Security Officer, hereinafter referred to as the Buyer and the first party, proposes to procure a Cyber Insurance Policy, hereinafter referred to as Services.
And
M/s……., represented by…… , Chief Executive Officer (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignee), hereinafter referred to as the Bidder/ Seller and the second party, is willing to offer/ has offered the Stores and / or Services.
2. Whereas the Bidder / Seller is a private company/public company /partnership/ registered export agency, constituted in accordance with the relevant law in the matter and the Buyer is a Public Sector Undertaking and registered under Companies Act 1956. Buyer and Bidder/Seller shall hereinafter be individually referred to as "Party" or collectively as the "parties", as the context may require.

3. Preamble

Buyer has called for tenders under laid down organizational procedures intending to enter into contract/s for supply / purchase / etc. of……and the Bidder / Seller is one amongst several bidders/Proprietary Vendor/Customer Nominated Source/Licensor who has indicated a desire to bid/supply in such tendering process. The Buyer values and takes primary responsibility for values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Seller(s).
In order to achieve these goals, the Buyer will appoint Independent External Monitor(s) (IEM) in consultation with Central Vigilance Commission, who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

4. Commitments of the Buyer.

4.1 The Buyer commits itself to take all measures necessary to prevent corruption and fraudulent practices and to observe the following principles: -
i) No employee of the Buyer, personally or through family members, will in connection with the tender, 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.
ii) The Buyer will during the tender process treat all Bidder(s) / Seller(s) with equity and reason. The Buyer will in particular, before and during the tender process, provide to all Bidder(s) / Seller(s) the same information and will not provide to any Bidder(s)/ Seller(s) confidential / additional information through which the Bidder(s) / Seller(s) could obtain an advantage in relation to the process or the contract execution.
The Buyer will exclude from the process all known prejudiced persons.

4.2 If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the Indian Legislation Prevention of Corruption Act 1988 as amended from time to time or if there be a substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer and in addition can initiate disciplinary action.

5. Commitments of the Bidder(s) / Seller(s).

5.1 The Bidder(s)/ Seller(s) commit himself to take necessary measures to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.
The Bidder(s)/ Seller(s) will not, directly or through any other persons or firm, offer promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in

exchange any advantage during the tendering or qualification process or during the execution of the contract.
The Bidder(s)/ Seller(s) will not enter with other Bidders / Sellers into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

The Bidder(s)/ Seller(s) will not commit any offence under the Indian legislation, Prevention of Corruption Act 1988 as amended from time to time. Further, the Bidder(s)/ Seller(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

The Bidder(s)/Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s)/ sub-contractor(s), if any. Further, the Bidder/Seller shall be held responsible for any violation/breach of the provisions by its sub-supplier(s)/sub-contractor(s).

5.2 The Bidder(s)/Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s)/ sub-contractor(s), if any. Further, the Bidder/Seller shall be held responsible for any violation/breach of the provisions by its sub-supplier(s)/sub-contractor(s).
5.3 The Bidder(s)/ Seller(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences

5.4 Agents / Agency Commission:
The Seller/Bidder confirms and declares to the buyer that the Seller/Bidder is the original manufacturer or authorized distributor / stockist of original manufacturer or Govt. Sponsored / Designated Export Agencies (applicable in case of countries where domestic laws do not permit direct export by OEMS) of the stores and / or Services referred to in this tender/ offer / contract / Purchase order and has not engaged any individual or firm, whether Indian or Foreign whatsoever, to intercede, facilitate or in any way to recommend to Buyer or any of its Functionaries, whether officially or unofficially, to the award of the tender / contract / purchase order to the Seller/Bidder; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller/Bidder agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in anyway incorrect or if at a later stage it is discovered by the Buyer that the Seller/Bidder has engaged any such individual / firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this contract / purchase order, the Seller/Bidder will be liable to refund that amount to the Buyer. The Seller will also be debarred from participating in any RFQ / Tender for new projects / program with Buyer for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract / Purchase order either wholly or in part, without any entitlement or compensation to the Seller/Bidder who shall in such event be liable to refund agents / agency commission payments to the buyer made by the Seller/Bidder along with interest at the rate of 2% per annum above LIBOR (London Inter Bank Offer Rate) (for foreign vendors) and Base Rate of SBI (State Bank of India) plus 2% (for Indian vendors). The Buyer will also have the right to recover any such amount from any contracts / Purchase order concluded earlier or later with Buyer.

6. Previous Transgression

6.1 The Bidder /Seller declares that no previous transgressions have occurred in the last three years from the date of signing of this Integrity Pact with any other company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprise in India that could justify Bidder's/ Sellers' exclusion from the tender process.
6.2 If the Bidder / Seller makes incorrect statement on this subject, Bidder / Seller can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason without any liability whatsoever on the Buyer.

7. Company Code of Conduct

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

8. Sanctions for Violation

8.1 If the Bidder(s)/ Seller(s), before award or during execution has committed a transgression through a violation of Clause 5, above or in any other form such as to put his reliability or credibility in question, the Buyer is entitled to disqualify the Bidder(s)/ Seller(s) from the tender process or take action as per the procedure mentioned herein below:

To disqualify the Bidder / Seller with the tender process and exclusion from future contracts.

To debar the Bidder / Seller from entering into any bid from Buyer for a period of two years.

To immediately cancel the contract, if already signed / awarded without any liability on the Buyer to compensate the Bidder /Seller for damages, if any. Subject to Clause 5, any lawful payment due to the Bidder/Seller for supplies effected till date of termination would be made in normal course.

8.2 If the Buyer obtains knowledge of conduct of a Bidder/ Seller or of an employee or a representative or an associate of a Bidder / Seller which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer.

9. Compensation for Damages

If the Buyer has terminated the contract according to Clause 8, or if the Buyer is entitled to terminate the contract according to Clause 8, the Buyer shall be entitled to encash the advance bank guarantee and performance bond/ warranty bond, if furnished by the Bidder / Seller, in order to recover the payments, already made by the Buyer for undelivered Stores and / or Services.

10. Price Fall Clause

The Bidder undertakes that it has not supplied/ is not supplying same or similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry/Department of the Government of India or PSU or Coal India Ltd and its subsidiaries during the currency of the contract and if it is found at any stage that same or similar product/ Systems or Subsystems was supplied by the Bidder to any other Ministry / Department of the Government of India or a PSU or any Public Sector Bank at a lower price during the currency of the contract, then that very price will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Buyer, if the contract has already been concluded."

11. Independent External Monitor(s)

The Buyer has appointed Independent External Monitors for this Integrity Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given in RFQ). As soon as the Integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the Independent External Monitors. The Bidder(s) / seller (s), if they deem it necessary, may furnish any information as relevant to their bid to the Independent External Monitors. If any complaint with regard to violation of the IP is received by the buyer in procurement case, the buyer shall refer the complaint to the Independent External Monitors for their comments / enquiry. If the Independent External Monitors need to peruse the records of the buyer in connection with the complaint sent to them by the buyer, the buyer shall make arrangement for such perusal of records by the Independent External Monitors. The report of enquiry, if any, made by the Independent External Monitors shall be Submitted to MD& CEO, National Bank for Financing Infrastructure & Development within 2 weeks, for a final and appropriate decision in the matter keeping in view the provision of this Integrity Pact.

12. Law and Place of Jurisdiction

This Integrity pact is subject to Indian Laws, and exclusive Jurisdiction of Courts at Mumbai, India.

13. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.
Integrity Pact Duration

14. This Integrity Pact begins when both parties have legally signed it. It expires for the successful Bidder / Seller 10 months after the last payment under the contract, and for all other Bidders / Sellers within 6 months from date of placement of order / finalization of contract.
If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by NaBFID.
Should one or several provisions of this Integrity Pact turn out to be invalid, the remainder of this Integrity Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

15. Other Provisions

15.1 Changes and supplements need to be made in writing. Side agreements have not been made.
15.2 The Bidder(s)/Seller(s) signing this IP shall not initiate any Legal action or approach any court of law during the examination of any allegations/complaint by IEM and until the IEM delivers its report.
15.3 In view of the nature of this Integrity Pact, this Integrity Pact shall not be terminated by any party and will subsist throughout its stated period.
15.4 Nothing contained in this Integrity Pact shall be deemed to assure the Bidder/ Seller of any success or otherwise in the tendering process.

16. This Integrity Pact is signed with NaBFID exclusively and hence shall not be treated as precedence for signing of IP with MoD or any other Organization.

17. The Parties hereby sign this Integrity Pact at_____on_____ (Seller/Bidder) and _____on_____ (Buyer)

BUYER	BIDDER* / SELLER*
Signature:	Signature:
Authorized Signatory	Authorized Signatory (*)
NaBFID Information Security department	
Date:	Date:
Stamp:	Stamp:
Witness	Witness
1._____	1._____
2._____	2._____

**Authorized signatory of the company who has also signed and submitted the main bid*

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

[Compliance to all line items is mandatory]

Sr No	Solution Capabilities	Compliance (Yes/No)
Cloud Based Secure Web Gateway/ Proxy		
1.	The solution must have a complete license for Web content filtering, Anti-Malware, SSL/TLS Inspection, Content Inspection, Advanced Threat Protection, Application Visibility and Control, Bandwidth Control, Visibility and Control of all ports and protocols, and Advanced Reporting with at least 1-year built in log retention.	
2.	The proposed solution must have the ability to handle all web and non-web traffic, across all ports and protocols, with infinite elastic scalability and unbeatable performance	
3.	The proposed solution must support policy creation based on defined criteria such as users, user groups, device trust status, geographic location, URL categories, cloud applications, destination IP addresses, custom URLs, and similar attributes.	
4.	The solution must support device posture of the endpoints prior to granting internet access as part of the proposed Zero Trust Architecture. The basic device posture checks should include a check for Microsoft Intune compliance, OS version, Host firewall status, Antivirus status etc. with provision to define custom check as well. The device posture checks must be supported in Android and IOS devices too	
5.	The solution must support comprehensive full inspection of both inbound and outbound internet traffic, including all versions of SSL/TLS-encrypted communications, regardless of port or protocol.	
6.	The solution must have the ability to create custom categories based on URLs	
7.	As a deterrent control, the solution must support user warning prompts/ caution message prior to access attempts to predefined websites.	
8.	The solution should be able to identify and block SSH and IRC tunneling attempts to prevent communication with Command and Control (C2) servers	
9.	The proposed solution should support both agent bases and agentless approach without compromising in the functionalities offered.	
10.	The proposed solution should enforce session blocking for certificates that are expired, issued by unrecognized authorities, have unresolved status, or encounter timeouts during validation etc.	

11.	The proposed solution should have the capability to create custom file-type control policies based on users, groups, type of applications, action type (upload and download) etc.	
12.	The solution must be capable of detecting and blocking phishing websites.	
13.	The proposed solution should have a dynamic risk scoring mechanism to evaluate the potential risk of the URLs accessed by the end users. It should support the auto-blocking of such high risk categorized URLs.	
14.	The proposed solution must have built-in Intrusion Prevention System (IPS) functionality for all web protocols like HTTP, HTTPS etc.	
15.	The proposed solution should support at least 5 devices (Laptop/ Desktop/ Mobile/ IPAD etc.) for a single authenticated user	
16.	The solution should support bandwidth throttling for large file downloads during business hours.	
17.	For effective utilization of the available Bank's network bandwidth, the proposed solution must provide the functionality for bandwidth caping based on users/ groups/ application accessed etc.	
18.	The solution should have an inbuilt DNS security solution to ensure safe browsing for end user.	
19.	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time.	
20.	The solution must be able to support XFF (XForwarded-For) to identify the source IP address of a host for effective correlation through SIEM.	
21.	The solution must feature a real-time threat intelligence and content filtering platform that includes regularly updated signatures and blacklists for high-risk categories such as phishing, malware, pornography, extremism, gambling, anonymizing services, C2 servers, ransomware, keyloggers, fraudulent websites etc.	
22.	The proposed solution must provide comprehensive web security that can identify and block malicious scripts (e.g., JavaScript, VBScript), executable files, unauthorized ActiveX controls, potentially unwanted programs, shareware, and cross-site content access.	
23.	The solution must enforce controls to restrict file uploads and downloads based on file type extensions and should intelligently detect and block files even if their extensions are altered or renamed.	
24.	The solution must support end-to-end encryption for data in transit, utilizing the latest industry-standard security protocols.	
25.	The solution must have the capabilities to inspect malware embedded in PDF, word, PPT files, etc.	
26.	The platform must support (allow/block/inspect) QUIC protocol, DoH, DoT etc.	

27.	The proposed solution must have the option to schedule automated backups within the admin console to create backups periodically without manual intervention to ensure compliance with the organization's Business Continuity Plans and Disaster Recovery Plans.	
28.	The solution must provide Role based access control (RBAC) for different user groups based on their job role for solution management.	
29.	The SSL/TLS Inspection platform must support inspection of different types of compression algorithms including nested compressed files.	
30.	The SSL/TLS inspection performed should be on real time basis and there must not be any latency induced by the SSL/ TLS inspection which will impact the end user experience.	
Cloud Access Security Broker (CASB)		
31.	The proposed solution must have the ability to auto discover, monitor, and control access to all popular cloud applications.	
32.	The solution must support the creation of detailed access control policies for Microsoft 365 applications (e.g., OneDrive, SharePoint, Teams), Google applications (e.g., Google Drive, Gmail, Google Doc) etc. including controls over file uploads, downloads, sharing, and security inspection.	
33.	The solution must support tenant (corporate vs personal tenants) base restrictions on the cloud web/ applications access.	
34.	The solution should have granular control over all popular social web applications like Facebook, LinkedIn, X(Twitter), YouTube, Instagram and others.	
35.	The solution must have the capability to create custom policies for Bank's cloud-based applications/ Web.	
36.	The solutions must have predefined cloud app (Microsoft Teams, CISCO WebEx, ZOOM, OneDrive, SharePoint, Google Drive etc.) policies for profiling and blocking.	
VPN/ Zero Trust Network Access		
37.	To strengthen overall security, the proposed solution should deliver consistent Zero Trust Network Access (ZTNA) for all users—whether they're connecting from the corporate LAN, branch offices via MPLS, or remotely—under a unified policy framework.	
38.	The proposed solution must have the ability to User-App-Segmentation in LAN for Office and Branch Users. Internal App traffic should not be sent to the Internet for LAN Users.	
39.	The solution should provide user to application segmentation and connect users to specific applications and limit lateral movement.	
40.	To eliminate the attack surfaces, the proposed solution must support application access through outbound service-initiated connections (unidirectional inside-out connections) i.e., it should not require any inbound firewall rule from OEM's cloud platform and only outbound traffic should be allowed.	
41.	The connectivity between the user's device and the private applications must be end to end encrypted and the traffic should	

	be optimally routed to the nearest data centers to ensure low latency.	
42.	The application publishers/ connectors must operate in high availability (HA) and support built-in load balancing.	
43.	The solution must support regular re-authentication of users or per app re-authentication after a certain configurable time period.	
44.	The proposed solution should support at least 5 devices (Laptop/ Desktop/ Mobile/ IPAD etc.) for a single authenticated user	
45.	The solution should have the ability to control access based on geolocation and must be able to block all traffic coming from hostile countries.	
46.	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time.	
47.	The proposed solution should be capable of providing secure private application access to all TCP and UDP based applications.	
48.	The endpoint agent must have inbuilt debugging capabilities.	
49.	The solution must be able to support XFF (XForwarded-For) to identify the source IP address of a host for effective correlation through SIEM.	
50.	The solution should enforce policies based on the following parameters but not limited to: • User • Group • User attributes (Roles, Departments etc) • User domains (e.g. corporate vs personal)	
Cloud Based Data Loss Prevention Solution		
51.	The proposed solution must have the ability to provide both Web based Data loss prevention and Endpoint level Data loss prevention.	
52.	The Solution must support the creation of DLP policies using parameters such as content, keywords, data patterns, metadata, file size, upload URLs, user groups etc. or any combination thereof.	
53.	There must not be any dependencies on the type/version of web browsers to enforce the DLP policies.	
54.	The solution must support the creation of DLP policies based on various data classification labels implemented through M365.	
55.	To enhance data protection, the solution should leverage AI and ML capabilities to analyze and understand sensitive content, including documents and images, and use sophisticated detection methods to safeguard against web-based data leaks.	
56.	The solution must block users from performing upload/downloads based on file type, document classification labels, file size etc.	

57.	The proposed solution must have predefined templates to identify PII data classifiers like, PAN, Aadhar, Card BIN, Account No , Voter ID Card No etc., IP	
58.	The proposed solution should give a prompt for user if any violation of DLP policies are flagged. Feature for capturing the justification from the end users must be incorporated in the prompt.	
59.	To prevent unauthorized data transfer, the Endpoint DLP must offer USB Device Control, enabling admins to enforce policies based on device attributes such as manufacturer, model, serial number, and device ID, and assign rules per user or group.	
60.	The solution must provide Content inspection for data movement to peripheral devices like USB, printers etc. with allow, block, User Alert actions etc.	
61.	The solution must support offline enforcement of Endpoint DLP policies, with comprehensive device control over USB, printer access, LAN connectivity, and Bluetooth communication etc.	
62.	The proposed solution must support advanced features like OCR, AI/ML, fingerprinting to safeguard organizations from various means of data leakage.	
63.	The solution must support time-bound DLP exclusions, allowing administrators to grant temporary exclusions that automatically expire after a specified duration.	
64.	The solution must enforce the DLP policies against the exclusion given for external sharing for one-drive in M365 to prevent Data loss.	
65.	The proposed solution must seamlessly restrict the sharing of sensitive data using various platforms like Microsoft email exchange, Microsoft Teams, Microsoft OneDrive, Microsoft SharePoint etc.	
Administration, Management & Reporting (Secure Web Gateway, VPN/ ZTNA, DLP)		
66.	The proposed solution must be able to integrate with Bank's on-premises Active Director (AD)	
67.	The solution must be able to integrate with SAML 2.0 (Azure AD, OKTA and ADFS etc.).	
68.	The solution must have the support for multi factor authentication for login to admin console.	
69.	To get better granular and easily readable reports, the proposed solution must provide minimum 1 year log retention period within OEM's platform for each web transaction.	
70.	For advanced analytics and forensic purposes, the proposed solution must provide at least 90 days of globally correlated real-time interactive reporting for every web transaction.	
71.	To troubleshoot critical performance related issues faster, the proposed solution must provide the proxy latency and server response time for every web transaction as part of its reporting.	
72.	The proposed solution must have the ability to do every transaction level logging (not summarized logging) with detailed information	

	including but not limited to: Timestamp, User Agent, Source IP, Destination IP, User, Destination Port, Applications, URL, URL Category, Policy Action etc.	
73.	The solution should have the ability to schedule the executive summary reports based on Bank's requirement.	
74.	The solution must provide complete audit trail logs for all the admin activities.	
75.	The solution should be capable of generating granular level custom reports such as but not limited to: 1) Usage Report of Specific User/IP/Group based on Date/Time 2) Report for all users who have accessed a specific URL 3) Usages report based on Date & Time 4) Top service user 5) Most requested service, etc.	
76.	The solution must have advanced built-in packet capture capability for troubleshooting.	
77.	The solution must provide full reporting including malware behaviour and intent, indicators of compromise (IOCs), dropped files, PCAPs etc.	
78.	The proposed solution must have the ability to monitor internet-based SaaS applications as well as other custom internet-based destinations (e.g., websites, web-based apps, third party proxy etc.)	
79.	The solution should provide advanced threat dashboard to track the infection or threat history for User/IP with the ability to access all forensic evidence for past infections (at least 1 year)	
80.	The solution should be able to schedule reports and provide the flexibility to generate on demand reports in daily/weekly/monthly/yearly or specific range.	
81.	The solution should support custom report creation in Excel, pdf, etc.	
Availability (Secure Web Gateway, VPN/ ZTNA, DLP)		
82.	To guarantee uninterrupted business operations, the OEM must commit to a 99.999% availability SLA covering all in-line, non-in-line, integration, and reporting services, with no exceptions or exclusions.	
83.	The solution must provide advanced threat protection (ATP) capabilities with an uptime SLA of 99.999% for all traffic (all ports/protocols) without any third-party integrations.	
84.	The solution must commit to ensure minimum latency in processing encrypted traffic which is ideally <= (60 ms to 110 ms) on an hourly basis.	
85.	The endpoint agent in the proposed solution must support business continuity during cloud infrastructure outages by offering a disaster recovery mode. This mode should allow administrators to grant access solely to pre-approved business-critical internet applications for enrolled users, avoiding traditional fail-open or fail-close behaviour.	

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 RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made at _____ between:

NaBFID constituted under the National Bank for Financing Infrastructure and Development Act, 2021 having its headquarters at Mumbai (Full address to be mentioned) through its _____ Department (hereinafter referred to as "NaBFID" which expression includes its successors and assigns) of the ONE PART;
And
_____ having its registered office at _____ (hereinafter referred to as "_____" which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;
And Whereas
1. _____ is carrying on business of providing _____, has agreed to _____ for NaBFID and other related tasks.

For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information being referred to as the "Receiving Party" and the Party disclosing the information being referred to as the "Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER

Confidential Information and Confidential Materials:

"Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and / or agents is covered by this agreement

Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality obligations prior to Disclosing Party's disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.

"Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

Restrictions

Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party's "Concerned Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Concerned Person, sufficient to enable it to comply with all the provisions of this Agreement. If the Service Provider appoints any sub-contractor (if allowed) then the Service Provider may disclose Confidential Information to such sub-contractor subject to such sub-contractor giving NaBFID an undertaking in similar terms to the provisions of this clause. Any breach of this Agreement by Receiving Party's Concerned Person or sub-contractor shall also be constructed a breach of this Agreement by Receiving Party.

Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are: the statutory auditors of the either party and government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

Rights and Remedies

Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information and / or Confidential Materials, or any other breach of this Agreement by Receiving Party and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and / or Confidential Materials and prevent its further unauthorized use.

Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that Disclosing Party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

Suspension of access privileges
Change of personnel assigned to the job
Termination of contract

Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

Miscellaneous

All Confidential Information and Confidential Materials are and shall remain the sole property of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any

expressed or implied right to Receiving Party to disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.

Confidential Information made available is provided "As Is," and Disclosing Party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or willful default of Disclosing Party.
Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

In case of any dispute, both parties agree for neutral third party arbitration. Such arbitrator will be jointly selected by the two parties, and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in English language at Mumbai and in accordance with the provisions of Indian Arbitration and Conciliation Act 1996 or any Amendments or Re-enactments thereto. Nothing in this clause prevents a party from having recourse to a court of competent jurisdiction for the sole purpose of seeking a preliminary injunction or any other provisional judicial relief it considers necessary to avoid irreparable damage. This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.

Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.
If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.
The Agreement shall be effective from _____ ("Effective Date") and shall be valid for a period of _____ year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

Suggestions and Feedback

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "Feedback").

Both parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the Receiving Party. However, the Receiving Party shall not disclose the source of any Feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this _____ day of _____ (Month) 20__ at _____(place)
For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

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)