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 EXPANSION OF EMPANELLMENT OF IT & CYBER SECURITY SERVICE PROVIDERS (ITCSSP)

Ref: NaBFID / IS / RFP /01A dated November 12,2024

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
November 26, 2024, up to 1600 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	By invitation ONLY
3	Last date for requesting clarification/Queries	Up to 4.00 PM on 19th November 2024 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 26th November 2024
5	Address for submission of Bids	For email submission: rfp@nabfid.org
6	Date and Time of opening of Technical Bids	5.00 PM on 26th November 2024 *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

Part – I

Part II

Part I

1. Objective of the RFP

National Bank for Financing Infrastructure and Development (NaBFID) , an All India Developmental Financial Institution created by Government of India under parliament act, head quartered at Mumbai, invites Request for Proposal [RFP] from reputed Cert-In empaneled entities/ companies / firms / service providers who have proven experience in the field of work/consultancy related to Information Security, Information Technology, Cyber Security & Information System audit for empanelment of Information Technology & Cyber Security Service Providers (ITCSSPs) approximately for a period of three years at Bank's discretion.

NaBFID had done an empanelment of CERT In empaneled entities to provide various Information Security Consultancy Services to the Bank in the month of May 2024. This RFP seeks proposals from the Cert-In empaneled entities (other than those entities who are currently empaneled) as part of the expansion of the ITCSSPs/Consultants of the Bank, adhering to the Bank's requirement(s) outlined in this RFP.

The successful bidder(s) will be added to the existing list of empanelment of ITCSSPs and will be continued to be in the panel of the Bank to provide information security services if their Cert-In empanelment is in force. The moment they are de-empaneled from the Empanelment List of Cert-In, for reasons whatsoever, they would stand de- empaneled from Bank's panel also.

In case the empaneled ITCSSPs do not respond to the quotation / inquiry by Bank on three occasions or do not perform / execute the assignment during the validity of the empanelment, they can be delisted from the Panel by the Bank. The decision of the Bank will be final and binding to the Empaneled ITCSSPs.

The purpose behind this RFP is to seek a detailed technical proposal for empanelment of Information Technology & Cyber Security Service Providers (ITCSSPs) for consultancy services. The aim of the RFP is to solicit proposals from qualified bidders for undertaking assignments as mentioned in the scope of this RFP. Interested eligible bidders may download the RFP from NaBFID website ***https://www.nabfid.org***

The empanelment of ITCSSPs is proposed to be **for a period up to June 2027 .**This would be subject to satisfactory performance and periodical review, as desired by the Bank from time to time. The Bank reserves the right to de-empanel any empaneled ITCSSP during the empanelment period. Empanelment does not confer any rights on the bidders to necessarily receive assignments/jobs. The allocation of assignments/jobs will be at the sole discretion of the Bank based on commercial evaluation in individual projects/activities.

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, its employees, secondees and deputed 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 respect will be at the Bidder's risk and may result in rejection of the Bid.

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.

Skill set & Experience requirements for resources.

Through this empanelment, the empaneled bidders are required to provide resources with the following skill set and experiences, based on requirements in various projects during the empanelment period. Details of minimum educational qualifications, skill sets and experience required for various levels of resources is as given below.

Level 1 (L1) Experience of above 2 years and up to 4 years	Educational Qualifications: B. Tech/ B.E in EC or CS or IT or Graduation in Information Security or Cyber Security or MCA Minimum one of below Mandatory Certifications: CEH/LPT/ ISO 27001/22301/27701LA/LI/ITIL or Certifications as per Level 2 or Level 3 Experience: Minimum of 5 VA/PT or Minimum of 5 application security assessments or ITGC audits/reviews, Process Audits/Reviews
Level 2 (L2) Experience of above 4 years and up to 6 years	Educational Qualifications: B.Tech/B.E in EC or CS or IT or Graduation in Information Security or Cyber Security or MCA • At least one certification of L1 eligibility is compulsory. • At least one of below Mandatory certifications: CISM/CISA / CISSP / OSCP / OSCE/CCSP • Experience: Conduct of banking domain level assessment of 2 years.
Level 3 (L3) Experience of above 6 years	Educational Qualifications: B.Tech/B.E in EC or CS or IT or Graduation in Information Security or Cyber Security or MCA • At least one (1) certification of L1 eligibility is compulsory. • At least Two (2) of below Mandatory certifications: CISM/ CISA / CISSP / OSCP/ OSCE/CCSP. Experience: Previous experience in specialized services and Banking domain experience of minimum 3 years.

5. Scope of Work:

Types of present and future activities and services required by Bank are covered/defined in this RFP is illustrative and indicative but not exhaustive. The scope& deliverables may also undergo changes/updates due to implementation of new products, technology, projects, configuration requirements, business needs, legal and regulatory requirements etc. Vendors are expected to update and include additional relevant items in these activities to conform to global best practices and currently available knowledge base. Actual service, scope & deliverables shall be defined at the time of issuance of work/purchase order.

A. Broad Scope of Work:

1. Services on Information Security and Security & Privacy Certifications (ISO Etc.)
2. Assistance in implementation of IT/IS Project/s and Tools.
3. Assistance in drafting RFPs & conducting technical evaluation for various Information Security projects. – PMC RFP
4. Security Review/audits including Outsourced Activities and Third-Party Audits.
5. Technological Risk Assessment, Risk Profiling and Threat Perception of Assets, GAP Analysis, Third Party Outsourcing Activities etc.

6. Documentation – Policy, Process, Procedure, SOP Creation/ Review/ Modification etc. related to Information & Cyber Security.
7. Immediate Risk Mitigation Measures.
8. Vulnerability Assessment [VA].
9. Penetration Testing [PT].
10. Application Security Testing.
11. Creation & review of Secured Configuration Documents [SCDs].
12. Network Audit and Database Audits.
13. Cyber Security Audits.
14. Application Audits/ Website Audit.
15. Cyber Forensic Investigation.
16. Assistance in Training and Security Awareness.
17. Advanced Real Time Threat Intelligence services for Security Project Management and Services.
18. Assistance in Compliance to the master directions/ advisories/ audit reports from regulator & statutory bodies.
19. Vendor risk assessments.
20. General process audit & migration audits.
21. Threat hunting exercises.
22. Red Teaming exercise.

23a. Assistance in implementation/ adherence to various Cyber laws & DPDP.

23b. Assess, develop & review information security controls, standards, metrics that provide for KPI/KRI.

24. Phishing / Vishing exercises
25. Data Privacy framework creation and assessments

Any other Information Technology/ cyber security related activity as decided by the Bank during the empanelment period.

B. Detailed Scope of Work:

1. **Services on Information Security and Security & Privacy Certifications (ISO, etc.)**

   The primary objective of this activity is to implement and certify Information Security and Privacy Management (ISMS / PIMS) for a defined scope of work.

   - **Activities to be covered:**
     i. Develop and Implement Information Security Management System (ISMS) & Privacy Information Management System (PIMS) and obtain ISO 27001 /27701 certifications for Bank.
        - Baseline the current security & Privacy controls in the IT infrastructure.
        - Assess any existing processes against the defined ISMS/PIMS processes.
        - Compare these to business needs and best practices.
        - Define and document the ISMS/PIMS governance principles, policies, procedures, plans, measurement matrices etc.
        - Assist the identified coordinators to implement and operationalize ISMS/PIMS processes through training.

- Conduct ISMS/PIMS awareness sessions for Bank employees at regular intervals.
- Conduct internal audit in line with ISMS/PIMS implementation requirements.
- Support the internal teams with coordination for certification audit.

ii. The implementation must consider improving process maturity level, introducing any needed process required to fulfil the requirement and provide all necessary deliverables related to it.

- **Deliverables**

i. Proposed ISMS & PIMS System including:
   - Policies, Plans, Procedures and Guidelines
   - Structure
   - Metrics Reporting Framework

ii. Various Templates
iii. Tool Recommendations, if any
iv. High level strategy and plan for review of critical systems
v. Internal Audit report
vi. Corrective & Preventive Action Plans

2. **Assistance in implementation of IT/IS Project/s and Tools.**

- **Activities to be covered:**

i. Project Planning:
   a. Define objectives, scope, and deliverables.
   b. Conduct risk assessments.
   c. Create a detailed project plan.

ii. Tool Integration:
   a. Evaluate and integrate tools.
   b. Provide training for effective utilization.

iii. Compliance and Standards:
   a. Assess against industry standards.
   b. Align with frameworks (e.g., ISO 27001).
   c. Develop governance principles.

iv. Continuous Improvement:
   a. Establish monitoring and evaluation.
   b. Implement feedback mechanisms.
   c. Introduce process enhancements.

v. Documentation and Reporting:
   a. Develop comprehensive documentation.
   b. Establish reporting mechanisms.

- **Deliverables:**

i. Project plan and risk assessment.
ii. Tool evaluation reports and integration recommendations.
iii. Compliance assessment and governance documentation.

iv. Continuous improvement framework.
v. Comprehensive project documentation and progress reports.

3. **Assistance in drafting RFPs & conducting technical evaluation for various Information Security projects.**
   - **Activities to be covered:**
     a. Possess expertise in drafting RFPs and conducting technical evaluations for Information Security projects.
     b. Demonstrate proficiency in assessing a variety of Information Security projects.
     c. Conduct activities in line with global best practices and standards.
     d. Develop a defined process for managing the technical evaluation process.

   - **Deliverables:**
     i. Comprehensive RFP documents.
     ii. Technical evaluation reports.
     iii. Recommendations for project enhancements.
     iv. Documented process for technical evaluations.

4. **Security Review/audits including Outsourced Activities and Third-Party Audits.**
   - **Activities to be covered:**
     a. Vendor must possess skills to conduct security reviews/audits on various IT systems, applications, and outsourced activities.
     b. Conduct audits following structured methodologies and global best practices.
     c. Evaluate third-party security measures and outsourced activities.
     d. Implement a defined process for managing evidence collected during security audits.

   - **Deliverables:**
     i. Comprehensive security review/audit reports.
     ii. Summarized reports with timelines.
     iii. Evidence collected in a scientific manner.
     iv. Recommendations for security enhancements

5. **Technological Risk Assessment, Risk Profiling and Threat Perception of Assets, GAP Analysis, Third Party Outsourcing Activities etc.**
   - **Activities to be covered:**
     a. Vendor should possess expertise in conducting technological risk assessments and profiling.
     b. Evaluate threat perception of assets, including IT systems and applications.
     c. Perform GAP analysis to identify vulnerabilities and weaknesses.
     d. Extend assessments to third-party outsourcing activities.
     e. Implement structured methodologies and global best practices in the assessment process.

   - **Deliverables:**
     i. Comprehensive technological risk assessment and profiling reports.
     ii. Threat perception analysis for assets.

iii. GAP analysis reports highlighting vulnerabilities.
iv. Assessment findings related to third-party outsourcing activities.
v. Recommendations for risk mitigation and security enhancements.

6. **Documentation – Policy, Process, Procedure, SOP Creation/ Review/ Modification etc. related to Information & Cyber Security.**

   - **Activities to be covered:**
     a. Drafting new Policy, Processes, Procedure for Bank as per Bank/ Regulatory requirement
     b. Reviewing/Modification of Existing policy as per industry best practices
     c. GAP assessment
   - **Deliverables**
     i. Drafted Policy, Process & Procedures
     ii. GAP Assessment Reports

7. **Immediate Risk Mitigation Measures.**

   - **Activities to be covered:**
     a. Vendor must be capable of identifying and implementing immediate risk mitigation measures.
     b. Assess and address risks across various IT systems, applications, and infrastructure in the Bank.
     c. Execute risk mitigation in a structured manner, adhering to global best practices.
     d. Utilize methodologies and tools to swiftly respond to and mitigate identified risks.
   - **Deliverables:**
     i. Documented immediate risk mitigation measures.
     ii. Implementation reports outlining actions taken.
     iii. Analysis of risks mitigated in a timely manner.
     iv. Recommendations for ongoing risk management strategies.

8. **Vulnerability Assessment [VA]:**

   Bank expects an authenticated type but non-destructive vulnerability assessment to be carried out. Vendor should be able to cover a broad range of systems including but not limited to Operating systems (Windows, Linux, AIX, HP UX etc), Databases (MS SQL Server, MySQL, Oracle, DB2 etc), Web servers (WAS, Apache, Tomcat, IIS etc), Application servers, Network devices (Cisco, Juniper etc), Security devices (Checkpoint, Fortinet, CISCO, Array etc), Virtualization, Cloud environment, various security solutions and business applications like Core Banking, Treasury , ALM etc. The Security review should cover comprehensive assessment of technological, functional, processes associated with the systems and IT, Information and Cyber Security eco system associated with systems under the Activities to be covered: of such review. Vendors are expected to conduct the audit against the standard configuration document that bank has created,

as also the latest global standards and industry best practices. In case, any new asset is identified during project execution, vendor is expected to develop the checklist and conduct the assessment.

The purpose of the vulnerability assessment is to discover all systems on perimeter network or internet facing and to assess these systems for securities vulnerabilities. Vulnerability assessment shall attempt to determine vulnerabilities that may enable unauthorized logical access to protected system via the external network interfaces by a 'naive' intruder who has limited and/ or no previous knowledge of the Bank's network. The vendor will conduct vulnerability assessment against network and security infrastructure components to identify services in use and potential vulnerabilities present.

The assessment should check for various categories of threats including:

i. Unauthorized access into the network and extent of such access possible.
ii. Unauthorized modifications to the network and traffic flowing over network
iii. Extent of information disclosure from the network
iv. Spoofing of identity over the network
v. Possibility of denial of services
vi. Possible threats from malicious codes (viruses and worms etc.)
vii. Possibility of traffic route poisoning

- **Activities to be covered:**
  A. General aspects for all systems
     i. Access control and authentication
     ii. Network settings
     iii. General system configuration
     iv. Logging and Auditing
     v. Password and account policies
     vi. Patches and Updates

  B. Specific requirements for Server/OS Configuration Audit
     i. File system security
     ii. Account Policies
     iii. Access Control
     iv. Network Settings / Network Port / Network Access Details
     v. System Authentication
     vi. Logging and Auditing
     vii. Patches and Updates
     viii. Unnecessary services
     ix. Remote login settings

  C. Configuration Audit of Networking & Security Devices
     i. Access Control
     ii. System Authentication
     iii. Auditing and Logging
     iv. Insecure Dynamic Routing Configuration
     v. Insecure Service Configuration
     vi. Insecure TCP/IP Parameters

vii. System Insecurities
viii. Unnecessary services
ix. Remote login settings
x. Latest software version and patches
xi. Traffic Analysis

D. Database Configuration Audit
i. Database Account Authentication
ii. Password Policy
iii. Database Account Privileges
iv. Database Auditing
v. Database Logging and Tracing
vi. Database Network Access Mechanism
vii. Database Patching
viii. Database Files and Directories Permission
ix. Access control and authentication
x. Unnecessary services
xi. Remote login settings
xii. Patches and updates

E. Security configuration of desktops, laptops, tablet phones and mobile devices that are used by the business users can be performed on sampling basis as per Bank's requirements.

- **Deliverables**
  Individual report should be provided for each of servers, network devices, and other audited units. Recommend revised and new security configurations based on global best practices.

- **Territorial scope**
  Servers/appliance hosted at Bank premises as well as Third party / Cloud Service Provider locations.

9. **Penetration Testing [PT].**
   The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks. The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.
   Consultant shall perform application security testing, to identify security vulnerabilities in the Bank's applications that may be exploited by a user to obtain unauthorized access. This will also include identification of any configuration issues that may not have been possible to identify during traditional vulnerability assessment.
   Consultant shall use automated and manual testing techniques to exploit the weaknesses identified in the application logic, in areas like authentication, authorization, information leakage, field variable control, session timeout & logout, cache control, serve side logic, client-side logic, error handling, application administration and encryption.

The Scope for penetration testing should include but not limited to list of internet facing websites/ applications in System Detail section.

It is explicit that penetration tester should conduct vulnerabilities assessment consulting with concerned personnel and proper permission of the Bank. Finally, remediation and recommendations must be provided along with all findings.

The following areas are to be considered for penetration testing:

i. Network Security:
   a. Password Security Testing
   b. Router Security Assessment
   c. Anti-Virus System Security Assessment and Management Strategy
   d. Internet User Security

ii. Host Security:
   a. Unix/Linux System Security Assessment
   b. Windows System Security Assessment
   c. Web Server Security Assessment
   d. Other relevant/mapped application Security Assessment

iii. Database Security Assessment

- **Activities to be covered:**
  a. Tests for default passwords
  b. Tests for DOS vulnerabilities
  c. Test for directory Traversal
  d. Test for insecure services such as SNMP
  e. Check for vulnerabilities based on version of device/server
  f. Test for SQL, XSS and other web application related vulnerabilities
  g. Check for weak encryption
  h. Check for SMTP related vulnerabilities such as open mail relay
  i. Check for strong authentication scheme
  j. Test for sample and default applications/pages
  k. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
  l. Test for information disclosure such as internal IP disclosure
  m. Look for potential backdoors
  n. Check for older vulnerable version
  o. Remote code execution
  p. Weak SSL Certificate and Ciphers
  q. Missing patches and versions
  r. This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

- **Deliverables**

  Detailed technical Penetration Test report should be provided which should contain:

  i. Executive Summary – Summarize the scope, critical findings, the positive security aspects identified in a manner suitable for the management.

ii. Categorization of vulnerabilities based on risk level – The report should classify the vulnerabilities as High/Medium/Low based on the Impact and Ease of Exploitation.
iii. Details of the security vulnerabilities discovered during the review – The detailed findings should be brought out in the report which will cover the details in all aspects.
iv. Solutions for the discovered vulnerabilities – The report should contain emergency quick fix solutions and long-term solutions based on industry standards.

- **Territorial scope**

Servers/appliance hosted at Bank premises as well as Third party / Cloud Service Provider locations.

10. **Application Security Testing.**

- **Activities to be covered:**

A. Technical Assessment
   a. The assessment should cover both business logic and technical risks.
   b. The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the application both from a business and technical aspect.
   c. The tester should attempt to identify and exploit vulnerabilities that include the WASP Top 10, including:
      - Input validation
      - Cross site scripting
      - SQL and XSL injection
      - Cookie modification
      - Code execution
      - Buffer overflow
      - URL manipulation
      - Authentication bypass
      - File upload vulnerabilities
      - Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
      - Session hijacking
      - CSRF
      - Privilege escalation
   d. The report should show risk to the business based on any exploits found.
   e. The assessment report should contain a test plan that shows what tests were conducted and its status.

B. Process Assessment
   a. Authorization and Segregation of Duties Controls
      - Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
      - Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).

- Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- Populate issue and findings log with the gaps / deviations issues noted (if any)

b. Assessment of Role based Security for Applications under scope
   - Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
   - Review of privileged access rights granted to application, system administrators, service providers and vendors
   - Assess the process for review of user logs for administrator and system users
   - Review ongoing monitoring of effectiveness of implemented procedures and controls
   - Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel.
   - Review of account and password policy including controls such as
   - Users are assigned unique accounts
   - Adequate passwords are maintained e.g. alphanumeric, minimum number of characters. etc
   - Periodic password changes and preventing repeated use of passwords and review of Implementation of password policy at system and application levels.

c. Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
   - Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles/ profiles.
   - Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
   - Perform sample testing of application's entitlements to confirm appropriate segregations of duties are being enforced by the system (in a test environment).
   - Understand how unsuccessful access attempts to applications in scope are logged and monitored
   - Review the implementation and effectiveness of user access management in applications in the event of leaves.
   - Review the segregation of development, production and test environments of applications

C. Others

a. Review the audit trail features of the applications in scope, understand how the audit trail reports are reviewed by Bank to detect errors and understand how the reported errors are corrected in a timely manner.
b. Review the maintenance and storage of audit trails and logs in order to assess whether the same can be used for forensic study if required by Bank
c. Understand the legal and statutory requirements related to using the applications in scope

d. Review other related procedures namely backup, change management, Escrow arrangement for source code and risk management processes for the applications in scope.

- **Deliverables**
  i. Identified threats for each application.
  ii. Report of findings and recommendations for each application.
  iii. All the reports would be prepared module/functionality-wise keeping the following points in view:
    - The assurance that application functions as intended by Bank's information security policy
    - Identification of gaps/ deviancies/ deficiencies/ vulnerabilities/ risks and detailed observations and its potential impact on the business
    - Industry best practices
    - Specific recommendations for improvement
    - Adequate verifiable audit evidences
  iv. Security and control review report of the applications in scope
  v. All observations will be thoroughly discussed with team/application owners before finalization of report and the users' views/explanations to be noted for deviations/recommendations. However, this should not influence the independent views/observations of the auditors.
  vi. All the documents and audit evidence, documentary or otherwise with screenshots/gist of discussion with stakeholders

11. **Creation & review of Secured Configuration Documents [SCDs].**
- **Activities to be included:**
  a. Vendor should possess expertise in creating and reviewing Secured Configuration Documents (SCDs).
  b. Conduct thorough reviews across various IT systems, applications, and infrastructure in the Bank.
  c. Implement structured methodologies following global best practices for SCD creation and review.
  d. Utilize appropriate tools to handle the creation and review process.
- **Deliverables:**
  i. Comprehensive Secured Configuration Documents.
  ii. Detailed review reports highlighting strengths and areas for improvement.
  iii. Updated SCDs with recommended enhancements.
  iv. Documentation of the creation and review processes.

12. **Network Audit and Database Audits.**
- **Activities to be included:**
  a. Vendor must possess expertise in conducting network audits and database audits.
  b. Perform comprehensive audits across various IT systems, applications, and infrastructure in the Bank.

c. Conduct audits in a structured fashion, adhering to global best practices.
d. Utilize methodologies and tools for effective network and database audits.

- **Deliverables:**
  i. Detailed network audit reports.
  ii. Comprehensive database audit reports.
  iii. Summarized reports with key findings and recommendations.
  iv. Evidence collected during audits in a scientifically documented manner.

13. **Cyber Security Audits.**

- **Activities to be included:**
  a. Vendor should have expertise in conducting cyber security audits.
  b. Perform comprehensive audits across various IT systems, applications, and infrastructure in the Bank.
  c. Conduct audits in a structured manner following global best practices for cyber security.
  d. Utilize methodologies and tools for effective cyber security audits.
- **Deliverables:**
  i. Detailed cyber security audit reports.
  ii. Summarized reports outlining key findings and recommendations.
  iii. Evidence collected during audits in a scientifically documented manner.
  iv. Recommendations for improving overall cyber security posture.

14. **Application Audits/ Website Audit.**

- **Activities to be included:**
  a. Vendor should possess expertise in conducting audits for applications and websites.
  b. Perform thorough audits across various IT systems and infrastructure in the Bank.
  c. Conduct audits in a structured manner following global best practices for application and website audits.
  d. Utilize methodologies and tools for effective audits.
- **Deliverables:**
  i. Detailed application and website audit reports.
  ii. Summarized reports with key findings and recommendations.
  iii. Evidence collected during audits in a scientifically documented manner.
  iv. Recommendations for enhancing application and website security.

15. **Cyber Forensic Investigation.**

The vendor should be able deploy personnel who can conduct forensic analysis on demand basis and help bank to conduct forensic analysis activities.

- **Activities to be included:**
  a. The vendor should have skill set to handle the forensic analysis activities across various IT systems, applications and infrastructure systems in the Bank.

b. Vendor should conduct the activity in a structured fashion using global best practices for conducting forensic analysis. Methodologies and tools should be handled by the vendor for handling the forensic analysis.
c. Vendor should have defined process for the management of the evidence that are collected during the forensic analysis

- **Deliverables**

  Deliverables should include detailed analysis reports, summary reports with timelines, evidence collected in scientific manner, etc as required in forensic analysis activity.

16. **Assistance in Training and Security Awareness**

- **Activities to be included:**
  a. Vendor should provide expertise in delivering training sessions on Information / Cyber security and Data Protection/Privacy.
  b. Conduct comprehensive training programs across various IT systems, applications, and infrastructure in the Bank.
  c. Implement training in a structured fashion using global best practices for security awareness.
  d. Utilize methodologies and tools for effective training and awareness programs.

- **Deliverables:**
  i. Detailed training materials.
  ii. Reports summarizing the effectiveness of training sessions.
  iii. Evidence of participation and engagement.
  iv. Recommendations for ongoing security awareness improvements.

17. **Advanced Real Time Threat Intelligence services for Security Project Management and Services.**

- **Activities to be included:**
  a. Vendor should provide advanced real-time threat intelligence services.
  b. Deploy personnel with expertise in threat intelligence across various IT systems and infrastructure in the Bank.
  c. Implement threat intelligence services in a structured fashion following global best practices.
  d. Utilize methodologies and tools for handling real-time threat intelligence in security project management and services.

- **Deliverables:**
  i. Comprehensive real-time threat intelligence reports.
  ii. Summarized reports with key insights and timelines.
  iii. Evidence of identified threats documented in a scientific manner.
  iv. Recommendations for proactive security measures and project enhancements.

18. **Assistance in Compliance to the master directions/ advisories/ audit reports from regulator & statutory bodies.**

- **Activities to be included:**
  a. Vendor should assist in ensuring compliance with master directions, advisories, and audit reports from regulators and statutory bodies.
  b. Deploy personnel with expertise in regulatory compliance across various IT systems and infrastructure in the Bank.
  c. Implement compliance activities in a structured fashion, following global best practices.
  d. Utilize methodologies and tools for effective compliance management.

- **Deliverables:**
  i. Documentation of compliance activities.
  ii. Reports summarizing adherence to master directions and advisories.
  iii. Evidence of compliance measures in a documented manner.
  iv. Recommendations for continuous improvement in compliance processes.

19. **Vendor risk assessments.**

- **Activities to be included:**

  Outsourcing of critical functions related to IT and Business should be assessed on periodic basis. The review should cover security control areas like Physical Security, Email Security, Logical Access control, Business continuity, Change management, Incident management, Media handling, Vendor governance, Network security, Systems security, Legal & compliance and each vendor should be assessed based on applicability of the controls. Assessment checklist should also cover server & desktop assessment on sampling basis, which are used for processing of bank's data. The assessment should also include:

  a. To access Information Security Risk in Outsourced Vendor Operations
  b. To conduct risk assessment of all outsourced vendors carrying out key operational processes for Bank vis-a-vis ISO 27001 standard
  c. To assess whether outsourced vendors meet/incorporate adequate level of security controls commensurate with the business information they receive/ store/process from or on behalf of Bank
  d. To assess whether the outsourced vendors comply with the IS Policy of the organization wherever applicable
  e. To assess adequacy of privacy and data protection controls at vendor premises

- **Deliverables**

  Formats, Templates and Reports on the above areas with recommendations.

20. **General process audit & migration audits.**

Assess whether the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security.

- **Activities to be included:**
  a. Assess the controls implemented in the system for: Input, Processing, Output, Functionality.
  b. Logical Access Controls - Review all types of Application-Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements.
  c. Assess sufficiency & accuracy of event logging, adequacy of Audit trails, SQL command prompt usage, database level logging etc.
  d. Assess interface controls - Application interfaces with other applications and security in their data communication.
  e. Assess authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition.
  f. Assess Data integrity & File Continuity Controls
  g. Assess controls for user maintenance, password policies being followed are as per bank's IT& IS security policy with special attention to the use of hardcoded User Id & Password
  h. Assess controls for segregation of duties and accesses of production staff and development staff with access control over development, test and production regions.
  i. Review of all types of Parameter maintenance and controls implemented.
  j. Assess controls for change management procedures including testing & documentation of change.
  k. Identify gaps in the application security parameter setup in line with the bank's security policies and leading best practices.
  l. Audit of management controls including systems configuration/ parameterization & systems development.
  m. Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, Monitoring of outsourced operations.
  n. Review of customizations done to the Software & the SDLC Policy followed for such customization.
  o. Verify adherence to Legal & Statutory Requirements
  p. Provide suggestions for segregations of Roles/Responsibilities with respect to Application software to improve internal controls.
  q. Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of user profiles, assignment & use of Super user access.

r. Check the sufficiency and coverage of UAT test cases, review of defects & tracking mechanism deployed by vendor & resolution including re- testing & acceptance.
s. Backup/Fall-back/Restoration /Recovery & Restart procedures

The above should be done in consonance with standards like ISO 27001/ ISO 22301, PCI-DSS, Bank's IT & IS/Cyber Security policies, legal & regulatory requirements & global best practices.

- **Deliverables**

Detailed findings and recommendation report with solution

21. **Threat hunting exercises.**

- **Activities to be included:**

To proactively search through Bank's network to detect and isolate advanced threats that evade Bank's existing security solutions:

a. Log Collection
   - Collect logs from key log sources in co-ordination with the bank.

b. Analysis of Logs
   - Create use-cases correlation rules specific to client's environment and event sources.
   - Analyse logs for indicators of compromise such as Command and
   - Control (CAC) Channels, malicious IPs & websites, Geo·map analysis for presence of malicious programs.
   - Analysis of logs to identify anomalous behavior/suspicious events.

c. Confirmation
   - Review and confirm observations with the client's security team.
   - Eliminate false positives.
   - Review effectiveness of SOC to detect similar events.

d. Reporting
   - Report containing compromised hosts, malware infections, presence of bots, CAC communications and other indicators of suspicious activities.
   - Provide recommendations for corrective action plan
   - Vendor may deploy additional tools for conducting threat hunting. The tools deployed shall be used for the period of engagement.
   - Threat Hunting shall also address the following:
     - Detect anomalous attacks, especially low-and-slow attacks that may be happening
     - Identify if the attack was detected by SOC
     - If the SOC has detected the attack, then identify the reasons for no action being taken
     - If the SOC has not detected the attack, then identify if an existing correlation rule requires tuning or if a new correlation rule is required or if a new solution is required.

22. **Red Teaming exercise**

In order to put Bank's cyber security defense to the test, Bank intends to run a real-world scenario that's designed to measure how well organization's defensive and response capabilities will stand up against social, physical, network and application attacks from a simulated real-life adversary.

- **Activities to be included:**
  a. Recognizing security issues within the Bank
  b. Perform legal assessment on local/remote networks
  c. Examining an organization for weaknesses as through the eyes of an industrial spy or a competitor
  d. Social engineering
  e. Trusted systems testing
  f. Password Cracking
  g. Identification of possible weak points in physical and logical security
  h. Vulnerability Research and Verification (automated and manual)
  i. Competitive Intelligence
  j. Internal application Testing
  k. Exploit Research
  l. Security testing of Firewalls, ACL other security devices
  m. Identification of Rouge Devices
  n. Cyber war game
  o. Determining appropriate countermeasures to thwart malicious hacking
  p. Conduct simulated cyber-attacks on the bank's infrastructure
  q. Validate protections and monitoring around high-value systems
  r. Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks

- **Deliverables**
  i. A report presenting results & conclusions of the exercise, covering technical, process and policy issues with a series of industry best- practice recommendations
  ii. Review of results and feedback in a workshop setting, to build awareness and alignment among stakeholders, and a roadmap of measures to improve security & resilience in the future
  iii. Short-term tactical fixes for immediate remediation of any outstanding vulnerabilities within the tested environments
  iv. Vulnerability report with mitigation plan and recommendations
  v. Long-term strategic initiatives that will proactively thwart any potential repetition of vulnerabilities discovered during the exercise

23 (a) Assistance in implementation/ adherence to various Cyber laws

Provide consultancy to Bank with reference to various Cyber & Data Protection laws, regulatory directions etc and help bank in complying with these laws/ directions.

- **Activities to be included:**

a. Provide details with regard to its relevance/applicability, consequences, obligations, risks of non-compliance/penalties etc. of each provision of applicable Cyber Law
b. Perform assessment to identify gaps in Cyber Law compliance status of the Bank
c. Provide detailed plan for compliance.
d. Help Bank in compliance.
e. Perform assessment for compliance.

- **Deliverables**

i. Detailed assessment of Bank's pre-compliance status
ii. Detailed report on gaps vis-a-vis the reference Cyber Law
iii. Plan of action for filling the identified gaps
iv. Compliance check report

23 (b) Data Privacy framework creation and assessments

Activities to be included:

- Assess the statutory/regulatory frameworks affecting the Bank.
- Conducting a privacy risk assessment:
- Aggregate the data necessary for informed policy and procedure formation and revision.
- Help Bank in establishing an internal privacy task force or working group, including members of legal, government relations, IT/IS, sales, public relations/marketing communications and other relevant groups within the organization.
- Review of company collection, maintenance, security, use, disclosure to third parties, and prospective strategies.
- Classify information into general categories.
- Personally identifiable/non-personally identifiable
- Sensitive/non-sensitive Information subject to specific statutory/regulatory requirements
- Assess requirements domestically and abroad, in all relevant jurisdictions.
- mapping data flows
- Assist Bank in devising its privacy strategy.

Deliverables

- Report on mapping of data flows

- Assist Bank in devising its privacy strategy

24 Assess, develop & review information security controls, standards, metrics that provide for KPI/KRI.

- **Activities to be included:**
  a. Assessment of Information Security Controls, standard and metrics used in Bank against industry best practices.
  b. Detailed GAP assessment as per Bank/Regulator guidelines

- **Deliverables**
  i. Assessment Report with detailed supporting evidence
  ii. Recommendation in terms of short term and long-term implementations
  iii. Presentation and short videos for Management

25 Phishing/Vishing exercise

Activities to be included:

Phishing/Vishing simulation exercises to be conducted using any of the following methods, as per Bank's requirement.

E-Mail Phishing Simulation Exercise

- Creating Mock E-mails: Develop customized email templates based on identified phishing scenarios.
- Developing of look-alike website/portal.
- Choose landing page: Design a webpage to be redirected from the phishing. email and to capture the user information/ credentials in encrypted form.
- Categorize and prioritize the delivery mechanism.
- Testing the servers and filters: Check if the servers and filters are bypassed for simulation.
- Pilot Testing: Perform the pilot test by sending emails to selected employees.
- Launch the mock attack: deploy the main phishing assessment to the target users.
- Monitoring- for phishing email delivery, response to phishing email, progress of phishing campaign.

Phishing simulation exercise through Vishing

- Developing infrastructure for vishing attack.
- Creating Vishing Scenarios.
- Conducting Vishing exercise.
- Collect the information about vished users.

- Capturing of Vishing responses received from the targeted employee.
- Executables for Vishing attack need to be provided by the Bidder.
- Vendor shall arrange Server and other infrastructure for the exercise at their own cost.

Phishing simulation exercise through Mobile

- Developing look alike mobile application (Android and IOS) for phishing attack.
- Categorize and prioritize the delivery mechanism.
- Hosting the phishing mobile application for the exercise in Vendor's Location.
- Conducting Mobile Phishing exercise.
- Reports & Statistics: Generate the report at the end of simulation and presentation to Management.
- Identifying the susceptible users and targeted awareness communications to improve the awareness level of users.
- Capturing mobile Phishing responses received from the targeted employee.
- Executables for Phishing attack need to be provided by the Bidder.
- Vendor shall arrange Server and other infrastructure for the exercise at their own cost.

Deliverables

- A detailed report presenting results, key learning & conclusions of the exercise, covering technical, process and policy issues with a series of industry best-practice recommendations, response of the targeted employees (e.g. Delivered, opened, clicked etc.) and user data/ credential collected of employees through phishing simulation. The same may be required to be presented before Senior Management /Committee.
- Discussion of the drafted report with the Bank's team and capture the feedback.
- Review of results and feedback in a workshop setting, to build awareness among employees, and a roadmap of measures to improve awareness among employees.
- Progress report comparison to previous exercises in the year.
- Communication to all targeted employees through email for their response to phishing simulation exercise & future guidelines.
- Info Graphics of Key-indicators to identify phishing e-mail, present in the e-mail sent to targeted employees during the simulation exercise, to be provided within 3 days of completion of exercise.

Any other information/ cyber security related activity as decided by the Bank during the empanelment period.

- **Activities to be included:**
  a. Vendor should be flexible to undertake additional cyber security-related activities as directed by the Bank.

b. Adapt skill sets to handle diverse cyber security tasks that may arise during the empanelment period.
c. Execute activities with a structured approach, aligning with global best practices.
d. Address any other cyber security-related needs as specified by the Bank.

- **Deliverables:**
  i. Tailored reports and documentation for additional cyber security activities.
  ii. Summary reports outlining key insights and timelines.
  iii. Evidence collected during specific activities documented in a scientific manner.
  iv. Recommendations and findings related to the additional cyber security tasks assigned by the Bank.

Territorial scope for activities under SoW: The Territorial scope for various activities/projects under the Scope of Work (SoW) includes Bank premises and Bank's infrastructure hosted at Third party /Cloud Service Provider locations.

6. Project Management

Successful bidder(s) must appoint a Support Coordination Manager, immediately after receiving the empanelment communication/letter. The Coordination Manager should have direct experience of successful end to end implementation/management of all activities throughout the empanelment period. The Coordination Manager should be directly and easily accessible to the Bank officials through convenient communication channels – phone/e-mail.

Detailed Project review must be conducted during project execution at no additional cost. These reviews are required weekly with the project leaders/ project manager or steering Committee level (of successful bidder and the Bank) respectively. The review will be in order to monitor progress of the project and take necessary corrective action, if required.

7. Technical Scoring Criteria

#	Technical Scoring Criteria	Maximum Score	Bidder's claim
1	Annual Turnover of the bidder in the last three financial years (i.e., 2020-21, 2021-22 & 2022-23) (For evaluation purpose, average of three years turnover will be considered) • >300 Crore: 15 Marks • >200 to < = 300 Crore Turnover: 10 marks • 100 to <=200 Crore Turnover: 5 marks	15	
2	No. of Years of experience of the firm in Information Security/ Cyber Security related activities in India in BFSI Sector.	10	

	(Evidence of the 1st assignment to be enclosed as a proof of experience /experience will be counted from the date of most relevant evidence) • >9 Years: 10 Marks • >7 to <=9 Years: 7 marks • > = 5 to <=7 Years: 5 marks		
3	Number of assignments carried out related to Information Technology/Information Security/ Cyber Security Activities for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP. Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence)	10	
4	Number of assignments related to projects in implementation of ISO 27001/ ISO 22301/ ISO 27701 for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP. Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence to be submitted as evidence)	10	
5	Skilled Employees / Resources on role with an experience of more than 2 years related to Information Technology, Information Security & Cyber Security domains. • 501 and above Employees: 20 Marks • 201 to 500 Employees: 15 Marks • 101 to 200 Employees: 10 Marks (Declaration on official letter head signed by competent authority to be submitted) **Designation** wise (Consultant /Sr Consultant/ Manager etc) and **domain** wise (IT, Information & Cyber Security) **count** of resources with minimum experience of 2 years in the reporting domain to be mentioned in the declaration.	20	
6	Number of assignments related to drafting of RFPs & conducting technical evaluation (end to end from RFP drafting till project finalization) / IT or IS project management / Migration audits for IT/IS projects in BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP.	10	

	Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence)		
7	Presentation to be made by the Bidder on understanding of requirements in the RFP including but not limited to: • Understanding of the objectives of the activities in the RFP • Bidder's approach, methodology and work plan • Relevant experiences • Proposed Team structure and Governance	25	
Total Marks		100	

The bidders who fulfill all the eligibility criteria and score a minimum of 70% in the technical evaluation will be shortlisted for empanelment. In case during technical evaluation, all the bidders fail to score more than 70% marks, or less than two bidders obtain more than 70% marks, then at Bank's discretion, the minimum scoring criteria may be reduced to 60%. 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.

8. 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.

9. 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.

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

a) A bidder requiring any clarification on RFP may notify NaBFID in writing strictly as per the format given in Annexure L by email within the date / time mentioned in the Schedule of Events.
b) A pre-Bid meeting will be held online on the date and time specified in the Schedule of Events which may be attended by the authorized representatives of the Bidders interested in responding to this RFP.
c) 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.

d) NaBFID reserves the right to amend, rescind or reissue the 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 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.

e) 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.

f) Queries received after the scheduled date and time will not be responded to/acted upon.

11. Contents of Bid Document:

a) The Bidder must thoroughly study / analyze and properly understand the contents of this RFP, its meaning and impact of the information contained therein.

b) 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.

c) 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.

d) 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.

12. BID Preparation & Submission:

a) Documents related to the bidding are to be submitted offline in sealed cover at NaBFID office. Parallelly, bidders are required to send the scanned copies of all such documents on

rfp@nabfid.org with signature of authorized signatory and official stamp of the organization by the date and time mentioned in the schedule of events.

b) Index of all the documents, letters, bid forms etc. submitted in response to RFP along with page numbers.

a) Bid covering letter / Bid form as mentioned in Annexure-A on Bidder's letter head.

b) Specific response with supporting documents in respect of Eligibility Criteria as mentioned in Annexure-B

c) Bidder's details as per Annexure - C on Bidder's letter head.

d) A copy of board resolution along with copy of power of attorney (POA or minutes of the partner's or authority letter wherever applicable) showing that the signatory has been duly authorized to sign the Bid document.

e) 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.

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

13. Modification and Withdrawal of Bids:

a) The Bidder may modify or withdraw its Bid after the Bid's submission, provided modification, including substitution or withdrawal of the Bids, is received by NaBFID, prior to the deadline prescribed for submission of Bids.

b) No modification in the Bid shall be allowed, after the deadline for submission of Bids.

c) No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP. Withdrawal of a Bid during this interval may result in appropriate action as per the terms of this RFP.

14. Period of Bid Validity:

a) Bid shall remain valid for a duration of 90 calendar days from Bid submission date or as may be extended.

b) 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.

15. 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.

16. Bid Security/ EMD (Refundable)

The bidder should deposit bid security of Rs.2,00,000/- (Rupees Two 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 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 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 M

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.

17. Awarding of contracts / Projects

Post empanelment of ITCSSPs, Bank will be inviting closed commercial bids from empaneled vendors (existing & newly empaneled) for individual projects during the empanelment period & contract will be awarded on L1 basis , from case-to-case basis, based on Bank's requirements. Such successful bidders shall submit Bank Guarantee for a value of 3% to 10% of the individual project/activity cost (TCO) (BG value will be decided case to case basis at the time of closed bidding)

with a claim period of 3 months post completion of the particular project period (case to case basis) as per the format mentioned in Annexure I.

In project executions (from time to time during the empanelment period), onboarded resources shall work from Bank premises (from its Mumbai Office) during Bank working days, unless the Bank agrees otherwise in the respective Work Order / purchase Order of a particular project.

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 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.

i. All pages of the bid shall be initialed by the person or persons signing the bid.

ii. Bid form shall be signed in full & official seal affixed.

iii. Any inter-lineation, erasure or overwriting shall be valid only if they are initialed by the person or persons signing the Bid.

iv. All such initials shall be supported by a rubber stamp impression of the Bidder's firm.

v. 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.

vi. 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

vii. 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 Bid

a. The Technical Bid should be complete in all respects and contain all information asked for in this document.

b. The following documents are to be submitted in original (in the order of precedence) to *Chief Information Security Officer, National Bank for Financing Infrastructure & Development, The Capital, A wing, 15th floor – 1503, G block, BKC, Bandra, Mumbai – 51* as well as by email (as a single pdf file with password protection) on or before last date & time of bid submission. The password may be shared in a separate email at the closing hours of bid submission.

i. Bid security of Rs.2,00,000/- (Rupees Two Lac only) in the form of a demand draft issued by a Scheduled commercial bank favoring National Bank for Financing Infrastructure & Development, payable at Mumbai or Bank Guarantee from scheduled commercial Bank with a validity for six months with claim period of 45 days.
ii. Annexure A – Bid form
iii. Annexure B – Eligibility criteria confirmation
iv. Company Registration proof
v. Evidence for Turn over compliance
vi. Evidence to prove Net worth
vii. Cert In empanelment proof
viii. Information Security/Information System audit proof (2)
ix. ISO certification exercise evidence (2)
x. RFP drafting experience proof (2)
xi. VAPT/App Sec review evidence proof (2)
xii. Red Team/Threat Hunting evidence proof (2)
xiii. Mumbai Office address in letterhead
xiv. Annexure B1 – Statement of resource details
xv. Annexure B2 – List of services & assignments in BFSI sector
xvi. Annexure B3 – Undertaking
xvii. Annexure C – Bidder details
xviii. Annexure D – Technical evaluation sheet along with evidence (if any, additional)
xix. Annexure E – Integrity Pact
xx. Annexure F -Undertaking regarding submission of PBG
xxi. Annexure G – Declaration of Compliance
xxii. Annexure H – Restrictions on procurement due to National Security
xxiii. Annexure I – Bid security declaration
xxiv. Annexure K – Certificate of waiver of MSE Firms , if applicable
xxv. Copy of the RFP & 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 empanelment process and Annexure L for pre bid queries ,if any. Further, empaneled bidders shall use Appendix I for Non-Disclosure Agreement, post completion of the

empanelment process & Appendix II for Performance Bank guarantee submissions, if any project is allotted to the bidder.

Non submission of 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 bidder's own risk and may result in the rejection of the bid.

c. 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.

d. Copies of relevant documents / certificates as proof in support of various information submitted in aforesaid annexures and other claims made by the bidder.

e. 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).

f. All the Annexures should be submitted in letter head of bidder duly signed with seal of the company. Photocopies of relevant documents / certificates as proof in support of various information submitted in aforesaid annexure and other claims made by the vendor.

g. Signed & Sealed copy of all the pages of RFP and corrigendum if any, to be submitted along with the technical bid.

h. 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.

i. The Bank reserves the right to resort to re-tendering without providing any reason whatsoever. The Bank shall not incur any liability on account of such rejection.

j. The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar features of a bidder.

k. The Bank reserves the right to modify any terms, conditions or specifications of RFP before date of submission of bids. Bidder has to submit bid documents as per the changes/modifications while submitting the bid. Notification of amendments/corrigendum will be made available on the Bank's website (nabfid.org), and will be binding on all bidders and no separate communication will be issued. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend

the deadline for a reasonable period as decided by the Bank for the submission of bids. No post bid clarification of the bidder shall be entertained.

21. Opening of Bids

TECHNICAL BID – Empanelment of Information Technology / Cyber Security Service Providers for NaBFID will be opened as per the schedule of this RFP. One representative of the bidder can be present for the opening of the Technical Offers. No separate intimation will be given in this regard to the bidders, for deputing their representatives.

However, Bids may be opened even in the absence of representatives of one or more of the Bidders. The Bank may, at its sole discretion decide to open the bid in the virtual presence of the representative of the bidders.

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

22. Bidding Document:

All pages of the Bid document should be serially numbered and shall be signed by the authorize person(s) only. The person(s) signing the bid shall sign all pages of the bid and rubber stamp should be affixed on each page except for a no amended printed literature. The bidder should submit a copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.

The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the Bidder's risk and may result in the rejection of its bid.

23. Erasures or Alterations

The original offer (Technical Offer) shall be prepared in indelible ink. There should be no hand-written material, corrections or alterations in the offer. Any such corrections must be initialed by the persons or person who sign(s) the proposals. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the forms using terms such as "OK", "accepted", "noted", "as given in brochure/manual" are not acceptable to the Bank. The Bank may treat non-adherence to these guidelines as unacceptable.

24. Rejection of Bid

The Bid is liable to be rejected if:

i. The document does not bear the signature of authorized person in each page and duly stamped.
ii. It is received after expiry of the due date and time stipulated for Bid submission.
iii. 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.
iv. It is evasive or contains incorrect information.
v. Any form of canvassing / lobbying /influence/ query regarding short listing, status etc. will be a disqualification.
vi. 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.
vii. Non-submission of bid security/EMD/Integrity Pact (IP).

25. 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 empanelment expansion of IT & Cyber Security Service Providers (ITCSSPs)" as per Annexure L

26. Technical Bid Evaluation

i. 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 email within three days or any such extended time frame informed, 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 their official mail boxes (as communicated to the Bank) in order to ascertain any clarifications are sought by bank post last date of bid submission. No separate intimation will be made by 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.

ii. 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.

iii. 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.

iv. All bidders will be required to give presentation of their offered services. Failure of a bidder to complete presentation to the Bank may result in rejection of the proposal. Bidder is required to address all queries raised by the Bank officials during the presentation. Giving mere presentation should not be considered as being qualified/shortlisted for further process. Decision of Bank, in this regard will be final and binding on all bidders.

v. Presentation should be made by the employee of the respective bidder firm as on bid submission date and no hiring of outsider for presentation will be allowed. The bidder is expected to substantiate /validate the achievements / recognition through relevant data / documentary evidence. Bidder should give presentation on the receipt of Bank's notice.

vi. Compliance of terms and conditions stipulated in the RFP duly supported by certified documentary evidence called for therein.

vii. The Bank reserves the right to evaluate the bids on technical & functional parameters including possible visit to inspect live site/s of the Service providers and witness demos, presentations or undertake a POC exercise of the system and verify functionalities, response times, user's acceptability etc.

viii. Marks for Technical evaluation will be awarded to the bidders as per the scoring criteria.

ix. All the eligible bidders will have to give a presentation in front of a committee constituted by the bank on a given date and time. All the presentations will be evaluated by the committee constituted by the Bank.

Technical scoring criteria with weightage of marks was briefed in earlier sections.

27. Contacting NaBFID:

i. No Bidder shall contact NaBFID on any matter relating to its Bid, from the time of opening of Technical Bid to the time the vendors are empaneled.
ii. Any effort by a Bidder to influence NaBFID in its decisions on Bid evaluation, bid comparison, or contract award may result in the rejection of the Bid.

28. Penalties:

Bank will be awarding work orders for different projects during the empanelment period post inviting closed commercial bids from shortlisted /empaneled bidders based on L1 criteria. Such selected bidders shall be liable to pay liquidated damages of 1% of the Work Order value, per week or part thereof for delay and not adhering to the time schedules of such work 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. 500/- per day of absence of L1 resource & Rs. 1000/- 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 Work Orders, the Bank reserves the right either to cancel the Work Order or to accept performance already made by the empaneled Applicant.

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.

It is pertinent to mention that Payment terms for different projects will be different based on the requirements.

29. Right to Verification:

NaBFID reserves the right to verify any or all of the statements made by the Bidder in the Bid document and to inspect the Bidder's facility, if necessary, to establish to its satisfaction about the Bidder's capacity / capabilities to perform the job. The Bidder to extend all necessary assistance in this regard, failing which NaBFID reserves the right to reject the Bid.

30. Right to Audit:

The Bidder 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 the 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 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.).

31. Sub-Contracting:

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

32. Limitation of Liability:

a) 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.
b) 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.
c) The limitations set forth herein shall not apply with respect to:
    i. claims that are the subject of indemnification pursuant to infringement of third-party intellectual property rights.
    ii. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,
    iii. damage(s) occasioned by Service Provider for breach of confidentiality obligations,
    iv. 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.

33. Confidentiality:

Confidentiality obligation of empaneled bidders shall be as per Non-disclosure Agreement placed as Appendix-I to this RFP document.

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.

34. Delay in Service Provider's Performance:

a) 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.
b) 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).

35. Service Provider's Obligation:

a) 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.
b) 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.
c) 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.
d) Service Provider is responsible for activities of its personnel and will hold itself responsible for any misdemeanors.
e) 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.
f) 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.
g) 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.

h) Service Provider shall ensure confidentiality, integrity, and availability of NaBFID's information at all times.

36. 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 / Work 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.

37. Conflict of Interest:

Bidder shall not have a conflict of interest (the "Conflict of Interest") that affects the bidding process. Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, NaBFID shall be entitled to forfeit and appropriate the security deposit as mutually agreed upon genuine estimated loss and damage likely to be suffered and incurred by NaBFID and not by way of penalty for, inter alia, the time, cost and effort of NaBFID, including consideration of such. Bidder's proposal (the "Damages"), without prejudice to any other right or remedy that may be available to NaBFID under the RFP and / or the Contract or otherwise.

38. Termination for Default:

a) 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:

   i. 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.
   ii. If the Service Provider fails to perform any other obligation(s) under the RFP / Contract.
   iii. Violations of any terms and conditions stipulated in the RFP / subsequent activity/project bid documents.
   iv. On happening of any termination event mentioned in the RFP / Contract.

b) 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.

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

39. Force Majeure:

a) 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.
b) 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.
c) 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.
d) 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.

40. 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.

41. Termination for Convenience:

a) 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.
b) 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.

42. 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.

43. 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.

44. Taxes and Duties:

a) 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.
b) 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.

45. 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

46 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.

47 **Contract Amendments:**

No variation in or modification of the terms of the Contract shall be made, except by written amendment, signed by the parties.

48. Bank's Right to Accept Any Bid and to Reject Any or All Bids:

The Bank reserves the right to accept or reject any Bid in part or in full or to cancel the bidding process and reject all Bids at any time prior to contract award, without incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Bank's action

49. Non-Transferable Offer

This Request for Proposal (RFP) is not transferable. Only the bidder who has submitted the bid will be eligible for participation in the evaluation process.

50. Intellectual Property Rights

The Bidder claims and represents that it has obtained appropriate rights to provide/use the Deliverables and Services upon the terms and conditions contained in this RFP.

The Bidder shall be responsible at its own cost for obtaining all necessary authorizations and consents from third party licensors of Software used by Bidder in performing its obligations under this Project.

If a third party's claim endangers or disrupts the Bank's use of the Deliverables, the Bidder shall at no further expense, charge, fee or cost to the Bank, (i) obtain a license so that the Bank may continue use of the Deliverables in accordance with the terms of this RFP.

Bidder shall indemnify and keep fully and effectively indemnified the Bank from all legal actions, claims, or damages from third parties arising outof use of software, designs or processes used by Bidder or his subcontractors or in respect of any other services rendered under this RFP.

51. Adherence to Standards

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.

52 RFP Ownership

The RFP and all supporting documentation are the sole property of NaBFID and should NOT be redistributed without prior written consent of the 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.

53 Proposal Ownership

The proposal and all supporting documentation submitted by the bidders shall become the property of NaBFID unless the Bank agrees to the bidder's specific requests, in writing, the proposal and documentation to be returned.

54 Tender/RFP Cancellation

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

55 Publicity

Any publicity by the Service Provider in which the name of the Bank is to be used, will be done only with the explicit written permission of the Bank.

Part II

Annexure –A

BID FORM (TECHNICAL BID)

[On Company's letter head]
(To be included in Technical Bid)

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 /01A dated November 12 ,2024.

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, favor, 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 2024

_____

(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 31, 2024.		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.100 Crores 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 / P&L statements 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 / Audited Balance sheet, Profit/ Loss statement of the firm to be provided of last three financial years.
4.	The bidder should be empaneled with CERT-In and should remain in panel during the currency of the contract.		Copy of the empanelment certificate to be submitted.

5.	The Bidder should have prior experience **(minimum one each)** from the assignments related to comprehensive security review as listed below for BFSI/Government/Regulatory firms in India during last five financial years from the date of this RFP: • Security Reviews including Third-Party Audits • Creation and Review of SCDs • Cyber Forensic Investigation • Training and Security Awareness		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof. *(The following information should be legible/ not masked in the evidence document : Name of the BFSI firm, Order date, Scope/Project details)*
6.	The Bidder should have at least 20 professionals having valid certification of CISSP / CISA /CISM/ OSCP /OSCE/ ISO 27001 LA /CEH as full-time employees and experience of at least five years in Information Security & Cyber Security domains.		Bidder may submit a certificate in its letterhead duly signed & sealed in **Annexure B1 format**
7.	Bidder must have carried out Minimum TWO (2) Information Security audit/ Cyber Gap Assessment/ IS Audit for BFSI/Government/ Regulatory firms in India during last 5 financial years from the date of this RFP.		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof.
8.	Bidder must have carried out Minimum TWO (2) assignments related to projects in implementation of ISO 27001/ ISO 22301/ ISO 27701 for BFSI/Government/Regulatory firms in India during last Five financial years from the date of this RFP		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof.
9.	Bidder must have carried out Minimum TWO (2) assignments related to Drafting RFPs and conducting Technical Evaluation /IT or IS project management / Migration audits for IT/IS projects for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP.		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof.

10.	Bidder must have carried out Minimum Two (2) Vulnerability Assessment and/or Penetration Testing (VAPT) and /or Application Security (APPSEC) for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP.		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof.
11	Bidder must have carried out Minimum TWO (2) Red Teaming and /or Threat Hunting activities for BFSI /Government/Regulatory firms in India during last Five financial years from the date of this RFP.		Submit Documentary Proof of Purchase Order / Work Order / contract copy / sign off / any other relevant document to establish the proof.
12	Bidder should have office presence in Mumbai		Office address with relevant details in official letter head to be submitted
13.	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs / FIs)		Submit an Undertaking in this regard in **Annexure B3 format**

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

Statement of details of resources with Experience & Certification

[On Company's letter head]

#	Resource identifier	Domain (IT/IS & CS)	Experience (in Years)	Professional Certification
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Annexure -B2

List of services & assignments in BFSI sector in India

#	Services/Assignments	Capability (Yes//No)	Total No. of Assignments
1	Vulnerability Assessment [VA].		
2	Penetration Testing [PT].		
3	Secured Configuration, & Hardening Documents Review - [Technical Standards Updation].		
4	Risk Assessment, Asset Classification, Review, Compliance of NDAs, SLA with Vendors / Third Party Outsourcing Agencies.		
5	General Controls Review / Audit Review and related Work.		
6	Anti-Phishing, Anti-Malware and Brand Monitoring Services etc.		
7	ISO 27001/22301/27701 related work		
8	Review, Update Gaps of Policies & Procedures viz. Information Security Policy , Cyber Security Policy, IS Audit Policy, CCMP, Information Security Procedures, IS Audit manual & Security KRIs		
9	IS Audit of infrastructure		
10	Forensic Audit / Analysis / Special Reviews / Scrutinize / Cyber Crime – Investigations and related Work.		
11	Evaluation of New Technology/Products against Industry Best practices and Information Security Controls		
12	Assess, Develop and Review Information Security Performance Dashboards focused on various measures such as effectiveness, ROI to convey value of investment on IS infrastructure across the Bank		
13	Assess, Develop and Review Information Security Controls, Standards, Metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.		
14	Data Governance, Data Privacy, Data Protection Strategy & Framework and Data Classification related Work.		
15	Develop, Implement, Training Information & Cyber Security Awareness, E-Learning Modules related to InfoSec related areas and Issues.		
16	Review of post-implementation of various IS initiatives and Project/s		

17	Security Risk Assessment		
18	Wireless Security assessment		
19	Cloud Security assessment		
20	Cyber incident response		
21	Red Teaming & Threat hunting exercise		
22	Social Engineering/Phishing Simulation		
23	Physical access controls and security assessment		
24	End to end onboarding process of SOC		
25	Any other relevant Assignment (Please mention)		

NOTE:

- In case of capability, experience and expertise vendors shall mention "YES" In case of "Capability" column kept blank, respective item no will be considered as NO.
- Kindly mention the No. of Assignments carried out in past three years (from RFP published date) against respective Sr. No.
- In case of ANY other related Activities NOT included in the above list, but related assignment/s carried out by the Bidder, may be added and included in the list after avoiding duplication along with the priority no. of such additional items.
- The information provided in the list must be supported by documentary evidence.

Signature
Seal of Company

Annexure B3

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-C

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 1.1. Name 1.2. Designation 1.3. Address 1.4. Phone Number (Landline) 1.5. Mobile Number 1.6. Email Address	

Name & Signature of authorized signatory

Seal of Company

Annexure-D

Technical evaluation Sheet

#	Technical Scoring Criteria	Maximum Score	Bidder's claim	Remarks/ Scoring statistics
1	Annual Turnover of the bidder in the last three financial years (i.e., 2020-21, 2021-22 & 2022-23) (For evaluation purpose, average of three years turnover will be considered) • >300 Crore: 15 Marks • >200 to < = 300 Crore Turnover: 10 marks • 100 to <=200 Crore Turnover: 5 marks	15		
2	No. of Years of experience of the firm in Information Security/ Cyber Security related activities in India in BFSI Sector. (Evidence of the 1st assignment to be enclosed as a proof of experience /experience will be counted from the date of most relevant evidence) • >9 Years: 10 Marks • >7 to <=9 Years: 7 marks • > = 5 to <=7 Years: 5 marks	10		
3	Number of assignments carried out related to Information Technology/Information Security/ Cyber Security Activities for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP. Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence)	10		
4	Number of assignments related to projects in implementation of ISO 27001/ ISO 22301/ ISO 27701 for BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP. Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant	10		

	document agreed by the Bank to be submitted as evidence to be submitted as evidence)			
5	Skilled Employees / Resources on role with an experience of more than 2 years related to Information Technology, Information Security & Cyber Security domains. • 501 and above Employees: 20 Marks • 201 to 500 Employees: 15 Marks • 101 to 200 Employees: 10 Marks (Declaration on official letter head signed by competent authority to be submitted) **Designation** wise (Consultant /Sr Consultant/ Manager etc) and **domain** wise (IT, Information & Cyber Security) **count** of resources with minimum experience of 2 years in the reporting domain to be mentioned in the declaration.	20		
6	Number of assignments related to drafting of RFPs & conducting technical evaluation (end to end from RFP drafting till project finalization) / IT or IS project management / Migration audits for IT/IS projects in BFSI /Government/Regulatory firms in India during last five financial years from the date of this RFP. Two marks per assignment for different activities/projects (Purchase Order/Work Order and sign off/ work completion confirmation or any other relevant document agreed by the Bank to be submitted as evidence)	10		
7	Presentation to be made by the Bidder on understanding of requirements in the RFP including but not limited to: • Understanding of the objectives of the activities in the RFP • Bidder's approach, methodology and work plan • Relevant experiences • Proposed Team structure and Governance	25		
Total Marks		100		

Annexure E

Integrity Pact

Tender Ref.No: NaBFID / IS / RFP /01A dated November 12,2024

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.

iii) 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.

i) 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.

ii) 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.

iii) 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.

iv) 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:

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

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

iii) 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

iv) 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

9.1 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)

11.1 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).

11.2 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.

11.3 The Bidder(s) / seller (s), if they deem it necessary, may furnish any information as relevant to their bid to the Independent External Monitors.

11.4 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.

11.5 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.

11.6 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.

14 Integrity Pact Duration

14.1 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.

14.2 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.

14.3 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 ……Division	
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 F

Undertaking of providing Performance Bank Guarantee

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,

Sub: **Undertaking for providing Performance Bank Guarantee –**Request for Proposal (RFP) For empanelment of IT and Cyber Security Service Providers.

We undertake to provide the Bank with a suitable Bank Guarantee in the format prescribed by the Bank under Request for Proposal (RFP), if any project/activity is allotted to us during the ITCSSP empanelment period , subject to successful empanelment of our firm.

Yours faithfully,

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

Date:

Annexure G

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 confirms to 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 H

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: _____

1. "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.)"
2. 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 I

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 Empanelment of Information Technology/Cyber Security Service Providers (ITCSSPs)

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:

1. If the bid submitted by us is withdrawn/modified during the period of bid validity.
2. 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.
3. In case of we becoming successful bidder and if:
   a) we fail to execute Contract within the stipulated time.
   b) we fail to furnish Performance Bank Guarantee within the timelines stipulated in this RFP document.

Yours faithfully,

Date:

For _____

Signature _____

Name _____

Authorized Signatories

(Name & Designation, seal of the firm)

Annexure J

LETTER FOR REFUND OF EMD

(To be submitted by bidders post completion of bidding 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) for Empanelment of Information Security/Cyber Security Service Providers (ITCSSPs) 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

Certificate of Waiver for MSE Firms, if applicable

(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 31.03.2020. 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 -L

Pre-Bid Query Format

(To be provide strictly in Excel format)

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

Appendix I

NON-DISCLOSURE AGREEMENT FORMAT
(For empaneled vendors, post completion of the empanelment activity, to be executed on Rs 500 stamp paper)

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.

2. 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

1. 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.

2. 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.

3. 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.

4. Miscellaneous

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

5. 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 during the empanelment period, against project/activity allotment)

Note:

1. This guarantee should be furnished by a Nationalized Bank / Scheduled Bank, as per the following format.
2. 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 Empanelment of Information Technology/Cyber Security Service Providers (ITCSSPs) _____(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 Empanelment of Information Technology/Cyber Security Service Providers (ITCSSPs) 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-transferrable.

Notwithstanding anything contained herein above:

1. Our liability under this bank guarantee shall not exceed **(3% - 10%) of the project cost.*(Bank will intimate the value at the time of awarding individual activity/project)***
2. This bank guarantee shall be valid up to _____.

3. 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)

Appendix III

Definitions & Abbreviations

The Bank	National Bank for Financing Infrastructure & Development
BE / Tech	Bachelor of Engineering / Bachelor of Technology
CEH	Certified Ethical Hacker
CISM	Certified Information Security Manager
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CS	Cyber Security / Computer Science
CSP	Cloud Service Provider
EC	Electronics & Communication
EMD	Earnest Money deposit
IS	Information Security
IT	Information Technology
ITGC	IT General Controls /IT Governance & Controls
ITIL	IT Infrastructure Library
LA /LI	Lead Auditor /Lead Implementer
L1/L2/L3	Level 1/Level 2 / Level 3
LPT	Licensed Penetration Tester
MCA	Master of Computer Application
OSCE	OffSec Certified Expert
OSCP	OffSec Certified Professional
PBG	Performance Bank Guarantee
TPSP	Third Party Service Provider
VA&PT	Vulnerability Assessment & penetration Testing