THE NEW INDIA ASSURANCE COMPANY LIMITED

Regd. & Head Office: New India Assurance Bldg.,
87, M. G. Road, Fort, Mumbai - 400 001.

e-Tender for Selection of Vendor for Verification of Regulatory Compliance, System Audit, VAPT, SCD & Info-Security Training

("NIA/HO/IS/05-2024/01")

Tender publishing date	06/05/2024, 10:00 Hrs
Last date of Bid Submission	27/05/2024, 15:30 Hrs
Date and Time of Technical Bid Opening	27/05/2024, 16:00 Hrs
Tender Fees (Non-Refundable)	**Rs. 5,000/-** ***(Rupees Five Thousand Only)***
EMD (Refundable)	**Rs. 2,00,000/- (*Rupees Two Lacs Only*)**
Address for Submission of Offline Documents	**CISO (Chief Information Security Officer)** **New India Assurance Co. Ltd,** **Fifth Floor, 87, M.G. Road, Fort,** **Mumbai-400001**
Contact Details	**Telephone No.:022-22708279/278** **Website : https://newindia.co.in** **e-ProcurementPortal: https://tenderwizard.com/NIAEPROC**
Last date of Queries	13/05/2024, 15:30 Hrs
Email ID for raising Queries	**E-mail id:** rfpnw.itho@newindia.co.in

INDEX

SECTION I

INSTRUCTIONS/GUIDELINES TO BIDDER

1.0) INTRODUCTION

The New India Assurance Company Limited (hereinafter referred as "The Company" or" New India "or" NIA"), India's premier General Insurance Company having a network of more than 2300+ Operating Offices spread across India. New India also has its presence in 28 countries across the globe.

Founded by Sir Dorabji Tata in 1919, NIA has been market leader in India in non-life insurance business for more than 40 years. NIA is the only direct insurer in India rated A- (Excellent – Stable outlook) by AM Best. "CRISIL has reaffirmed its ' AAA/STABLE ' rating on NIA indicating that the company has the highest degree of financial strength to honor its Policyholders obligations".

2.0) OBJECTIVE

New India intends to perform the comprehensive audit as per IRDAI issued information & cyber security guidelines released on 1st April'2023 and any other subsequent amendments to these guidelines or any new guideline released on Cyber Security which falls during contract period. Along with this, New India desires to carry out thorough System Audit.
Aside from this NIA intends to conduct vulnerability assessment & Penetration Testing for the network devices, security devices, various servers residing at the critical locations like the Data Centre (Rabale, Mumbai),Disaster Recovery site (Bangalore) & Near Disaster Recovery site (Airoli, Mumbai) etc., public facing websites, Critical API's security testing & various other applications to verify the controls in place.

Furthermore, NIA wants to create, Implement and review hardening guidelines for various information systems and Information Security Training for Employees, Senior Management & vendors.

Detailed scope is covered under **Section I 12.0)** scope of work.

3.0) INVITATION OF TENDER BIDS

The New India Assurance Company Limited invites bid through online mode of tendering (e-tender) from the interested and eligible bidders for above-mentioned requirements. The criteria and the actual process of evaluation of the responses to this tender and subsequent selection of the successful bidder will be entirely at Company's discretion.

This tender seeks proposal from Bidders who have the necessary experience, capability & expertise to conduct comprehensive audit as per IRDAI issued framework &industry standards, System Audit, Secure Configuration Documents implementation and review, Information Security Training and perform VA&PT (Vulnerability assessment & Penetration testing) in line with requirement of the Company as outlined in this tender (Refer Eligibility Criteria as per Annexure- I).

Note: - This tender is not an offer by New India, but an invitation to receive responses from the Bidders. No contractual obligation whatsoever shall arise from the tender process unless and until a formal contract is signed and executed by duly authorized official(s) of New India with the selected Bidder.

4.0) THE TENDER OFFER

4.1) The tender documents will be available on official web-site of NIA (https://newindia.co.in) as well as our E-Tender portal (**https://www.tenderwizard.com/NIAEPROC**).

4.2) The bidder has to use the E-Tender portal for participating in the tender (Refer Annexure-8 for e-tendering instruction).

4.3) Downloading of tender document from E-Tendering portal is mandatory for tender participation.

4.4) The online bids under two envelopes/ cover system comprising of (1) The technical bid and (2) commercial bid should be submitted online on E-Tender portal. Various documents to be submitted online and offline along with the technical and the commercial bid are as mentioned in the Section-II of this document.

4.5) If the last date for submission of offline documents happens to be a holiday due to some unforeseen circumstances, then the offline documents can be submitted by 11.00 AM on the next working day.

4.6) At any time prior to the last date of receipt of bids, the Company may, for any reason, whether at its own initiative or in response to clarifications requested by the prospective bidders, modify the tender document by clarifications.

4.7) The Clarifications, If Any, Issued By The Company At Any Time Before The Due Date Of Submission of the bid will become part of the tender document and would be notified on the official web-site of NIA (https://www.newindia.co.in/tender-notice) as well as at (https://www.tenderwizard.com/NIAEPROC).

4.8) No bid will be accepted after the due date & time.

5.0) EARNEST MONEY DEPOSIT (E.M.D)

5.1) The intending bidders should submit **Bank Guarantee** in favor of **"The New India Assurance Company Limited"** payable at Mumbai.

5.2) The Bank Guarantee should be from a nationalized bank and has to be valid for 180 days from the last date of tender submission. Bidders can use bank's standard Bank Guarantee format for submitting the EMD.

5.3) The bank guarantee should be irrevocable to the bidder during the validity period.

5.4) The EMD will not carry any interest.

6.0) FORFEITURE OF E.M.D

The EMD made by the bidder will be forfeited if –

6.1) The bidder withdraws the tender after acceptance.

6.2) The bidder withdraws the tender before the expiry of the validity period of the tender.

6.3) The bidder violates any of the provisions of the accepted terms and conditions of this tender specification.

7.0) REFUND OF E.M.D:

7.1) EMD will be refunded to the successful bidder, only after signing of the contract and submission of Security Deposit, completion of formality etc. in all respects to the satisfaction of the Company.

7.2) In case of unsuccessful bidders, the EMD will be refunded to them after intimation is sent to them about rejection of their tenders.

8.0) THE COMPANY RESERVES THE RIGHT TO

8.1) Accept / Reject any of the Tenders.
8.2) Add, Modify, Relax or waive any of the conditions stipulated in the tender specification wherever deemed necessary.
8.3) Reject any or all the tenders without assigning any reason thereof.
8.4) Award contracts to one or more bidders for the item/s covered by this tender.

9.0) REJECTION OF TENDERS:

The tender is liable to be rejected **interalia**:

9.1) If it is not in conformity with the instructions mentioned herein,
9.2) If it is not accompanied by the requisite EMD,
9.3) If it is received after the expiry of the due date and time,
9.4) If it is evasive or incomplete including non-furnishing the required documents.
9.5) If it is quoted for period less than the validity of tender.
9.6) If it is received from any blacklisted bidder or whose past experience is not satisfactory.
9.7) If the technical Bid doesn't fulfill the requirement.
9.8) If it is not properly signed by the bidder.

10.0) VALIDITY OF TENDERS

Tenders should be valid for acceptance for a period of at least 180 (One Hundred and Eighty) days from the last date of tender submission. Offers with lesser validity would be rejected.

11.0) SIGNING OF CONTRACT

The successful bidder shall sign and return the Agreement (**Annexure-7**) within 2 weeks from the date of purchase order/work order from NIA.

12.0) SCOPE OF WORK (SOW)

Phase-1

A) Assurance Audit of NIA's IT Infrastructure as per IRDAI framework on Information & Cyber Security

As per IRDAI guidelines & industry standards on information and cyber security for insurers, the bidder has to perform following activities:

- Comprehensive Assurance audit of NIA for Information Security/Cyber Security and according to Information and Cyber Security Guidelines V 1.0 Ref no. IRDAI/GA&HR/GDL/MISC/88/04/2023 released on 24th April'2023 (all the domains of circular have to be covered) and any other subsequent amendments to these guidelines or

any new guideline released on Cyber Security which falls during contract period. Auditor also has to follow amendments done in VAPT guidelines issued on 30-12-2020 Ref. NO.: IRDA/IT/CIR/MISC/301/12/2020.

- Audit will include scope and compliance as per above mentioned circular.
- The auditor has to refer IRDAI Audit Checklist of total 348 controls shared with the guidelines for audit.
- Review of preparedness/readiness of the NIA vis-à-vis IRDAI Circular on Cyber Security Framework.
- Auditor should be fulfilling eligibility criteria mentioned in Annexure IV of the IRDAI guidelines.
- Audit of the NIA's Current Cyber Security Architecture.
- The bidder has to provide recommendations to increase the effectiveness of the security controls.
- Knowledge Transfer during execution of the Assignment, provide documentation and material.
- The bidder would recommend improvements to better align the security architecture with business objectives, the NIA's information& cyber security policy and industry best practices.

Deliverables

- NIA would need separate comprehensive reports on all the aspects covered in the aforementioned scope of work.
- The report has to be formulated Category wise as defined in IRDAI document. It should incorporate methodology used, gaps identified, severity of gaps, possible issues that can occur, various risks which may arise, mitigation methods etc.
- Auditor has to share the report in format shared by IRDAI i.e. Annexure III.
- Auditor has to provide Certificate on Cyber security controls as per Annexure-5 of Information and Cyber Security Guidelines v 1.0 Ref no. IRDAI/GA&HR/GDL/MISC/ 88/04/2023 released on 24th April'2023. The detailed report of review should be as per Annexure A of Annexure -5 of the same guideline.
- Graphical representation outlining the as-is [current state] Enterprise information/cyber Security Architecture.
- Graphical representation outlining the to-be [future state] Enterprise information/cyber Security Architecture.
- The summary of cyber security readiness exercise and recommendations for improvement areas.
- A roadmap which includes prioritization of improvement areas.

Phase-2

B) System Audit

As part of this scope, the bidder has to perform comprehensive system audit for the following sections where process walkthroughs have to be done to understand the processes in place, risk areas have to be identified, design & operating effectiveness of the controls in place have to be evaluated, control gaps if any have to be identified and has to provide recommendations for improvement areas.

It will include 25-30 applications, no of IP's (around 280-300) that includes network devices, security devices, different servers, databases etc), approx. 20 API's workflow security review. The

scope will involve Third Party Administrator (TPA) risk assessment audit remotely which are approximately 16 in number, On-line and On-premise Vendor Risk assessment for vendors providing services remotely to NIA (For On premise audit - number of vendors sites outside Mumbai are approximately 3 in number in regions - Noida, Bangalore, Kolkata). The vendor has to submit a checklist for system audit domain covering all the parameters and following best cyber security practices, guidelines from ISO, IRDAI, RBI, NIST, SOC, Data Privacy etc.

The parameters for System Audit is mentioned below.

- IT Governance & Strategy
- High level system architecture review
- Information & Cyber Security policy & Procedures
- Assessment of in-scope business applications
- Data Center(DC), Disaster Recovery (DR) & NDR (Near Disaster Recovery) operations
- SDLC Audit
- Change Management
- Patch Management
- Access Management
- Asset Management
- IT Operations (Configuration management, Job scheduling, Backup & Restore etc)
- Data Security
- Network security
- Email Security
- Endpoint Security
- System Acquisition, Development & Maintenance
- Incident Management
- Database Security
- Mobile &Tele working Security
- Physical & Environmental Security
- Antivirus Controls
- TPA (Third Party Admin1strator) Risk Assessment (16)
- Vendor Risk Assessment
- Cryptography & Key management
- Virtualization
- Cloud Security
- Security Logging & Monitoring
- Audit Trails
- Data Privacy

Deliverables:

- NIA would need a comprehensive report on all the aspects for aforementioned areas.
- Network architecture review will involve planning, review of all deployments and submitting a Comprehensive report to NIA on how to improve and Consolidate Various Network Architectures.
- The report has to be formulated Category wise as per areas mentioned herein above. It should incorporate methodology used, gaps identified, possible issues that can occur, various risks which may arise, mitigation methods etc.
- Vendor Risk Assessment and TPA risk assessment reports should be a separate report from System audit report and will be vendor-wise.

Phase-3

C) Vulnerability Assessment& Penetration Testing

1) To check the robustness of the IT infrastructure, applications & identify vulnerabilities, the bidder has to perform vulnerability assessment and penetration testing (through grey box testing).

Grey Box Testing

1) It will include number of IPs (around 280-300), 25 API's and about 30 applications for the vulnerability assessment & penetration testing.
2) As per guidelines issued on 29-12-2020 Ref. NO.: IRDA/IT/CIR/MISC/301/12/2020 by IRDA the bidder has to perform Vulnerability assessment and penetration testing (through grey box testing) annually for Intranet applications (approx. 12-16) and once in 6 months for internet facing applications (approx. 12-14).

3) Every VA&PT testing will involve 2 cycles one at the beginning of VA&PT for identification of gaps and to check for known vulnerabilities, and a retesting post closure of vulnerabilities identified (Revalidation testing).

    i. 1st VA&PT for identification of gaps will include IP's about 280-300 in number, 25 API's and about 30 applications.
    ii. 2nd VA&PT for identification of gaps will include 12-14 internet facing application and Wireless controller & access points.

4) Revalidation Testing

    i. 1st Revalidation testing will be done for internet facing applications (approx. 12-14), 25 API's and Wireless controllers for access point after submitting initial report of 1st VA&PT Grey box testing for identification of gaps.
    ii. 2nd Revalidation testing will include all the 30 application, and IP's around 280-300 after the report of 2nd VA&PT Grey box testing for identification of gaps.

5) Timelines for completing 1st VA&PT Testing for identification of gaps and 1st Revalidation testing should be within 4 months and timeline for completing 2nd VA&PT Testing for identification of gaps and 2nd Revalidation testing should be within 4 months.

Black Box Testing

1) For closure of identified gaps in all internet facing applications and Infrastructure components, External Black Box Penetration Testing should be done within one month after receiving the 1st and 2nd VA&PT report respectively for identification of gaps.

VA&PT should be comprehensive that includes following activities:

- Network Scanning/Surveying
- Port Scanning
- Port sweep
- System & OS Fingerprinting
- System Identification & Trusted System Scanning

- Vulnerability Scanning
- Service Fingerprinting
- Secure Configuration Review

Website/application assessment should be done against all known vulnerabilities Including but not limited to latest OWASP vulnerabilities:

- SQL injection
- Broken Authentication and Session Management
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security Mis-configuration
- Insecure Cryptographic storage
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-Validated Redirects and Forwards
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Any other loopholes, which makes websites & applications vulnerable to malicious attacks.

API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities:

- Broken Object level authorization
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted resources consumption
- Broken function level authorization
- Unrestricted access to sensitive business flows
- Server side request forgery
- Security misconfiguration
- Improper inventory management
- Unsafe consumption of API's

- **Deliverables:**

- NIA would need a comprehensive report on all the aspects covered in the scope of work with detailed recommendations to plug the vulnerabilities.
- It should incorporate methodology used, gaps identified, possible issues that can occur, possible risks which may arise, mitigation methods etc.
- In case New deployments of API and Application is done the vendor has to perform VAPT at no additional cost to NIA.

Phase-4

D) Review and Creation of the hardening documents

Phase-4 (a)
The bidder has to review NIA's existing Secure Configuration Documents adopting best practices for server's OS, Database, Security Devices, Network Devices etc. & update the same in case of any gap.

Phase-4 (b) Also Bidder has to scan the whole environment and create new secure configuration documents if any for Windows OS for end devices, Server's OS, Database, security devices, Network devices etc. and ensure its implementation with the existing vendor. As per existing requirement Vendor has to create and implement 20 Documents. The cost mentioned for this phase is a Onetime requirement and if contact is extended by 1 more Year this cost will not be Considered.

Phase-4 (c) The vendor also has to quote a base price per document for the requirement over and above as mentioned in Phase -4 (b) i.e. if count exceeds 20 Documents.

Deliverables:

- NIA would need a comprehensive report on aforementioned aspects covered in the scope of work.
- It should incorporate methodology used, gaps identified, possible issues that can occur, possible risks which may arise, mitigation methods etc.
- The Vendor have to submit the Implementation report evidence for the new configuration document with all the details, e.g. (Plan, Use Case for NIA, Implementation checklist suggested and implemented).

Phase-5

E) Information Security Training to Employees, Vendors and Senior Management

- As part of the tender the Vendor has to provide Information Security Training to Employees and 4 Sessions will be arranged Annually where each session will cover 1 Region (North, South, East, West).
- Training to Vendor will be arranged on an annual basis. (1 Session in a Year)
- Senior Management training will be arranged twice a Year covering new threat vectors, Cyber security Hygiene etc.
- Training to NIA IT team and IS team.

Deliverables:

- The training shall be conducted both in offline and Online/Virtual mode as per NIA requirement.
- The content format for conducting Information/ Cyber Security Awareness Training program shall include the following:
  i. E-Mail content,

ii. SMS Content
iii. Web Content
iv. Quizzes
v. Manual/Booklets/Brochures
vi. Publishing Screen Savers across the NIA's End User Workstations from Cyber Security perspective.
vii. Cyber Security Awareness Sessions /Presentations [PPT]

- **Indicative list of Information/Cyber Security Awareness topics for Senior Management:**
  i. Cyber Security Basic Principles covering CS Basic terminologies, different frameworks and Security Governance.
  ii. Cyber Security as an enterprise-wide risk management issue covering Role of Business Heads in Cyber Security and the need of cyber security posture/preventive, detective, corrective controls
  iii. IT Risk management covering different types of Risks, key metrics, reporting structure and Risks mitigation measures.
  iv. Business Continuity Management [covering BIA, BCP and DRP etc.,]
  v. Cyber Security Framework [NIST, COBIT etc.,]
  vi. Current Trends and Techniques in Cyber Security environment
  vii. IT/Cyber Security Risk Management
  viii. Vendor Risk Management/ TPRM [Third Party Risk Management]
  ix. Social Engineering attacks
  x. Cyber Security Risks in Remote Working
  xi. Cloud Computing Security and challenges
  xii. Importance of Information Security / Cyber Security Policies, Guidelines
  xiii. Threat Intelligence Advisories like US-CERT, CSITE, CERT-In, MeITy etc.,
  xiv. IT Act 2000, 2008 IT Act amendment, Data Protection Bill (DPDP Act)
  xv. Any other latest topic/happenings related to cyber security

- **Indicative list of Information/Cyber Security Awareness topics for Employees:**
  i. Introduction to Cyber Security
  ii. Basic Cyber Security Terminology
  iii. Business Continuity Management
  iv. Incident Detection and Response
  v. Recent Cyber Security Breaches
  vi. Digital Payments and Security measures
  vii. Importance of Information Security / Cyber Security Policies, Guidelines
  viii. Any other latest topic/happenings related to cyber security
  ix. Latest topics related to IT/technology
  x. Hands-on sessions on above topics as per NIA's requirements

- **Indicative list of Information/Cyber Security Awareness topics for Vendors and NIA IT and IS team:**
  i. Basic Cyber Security Terminology
  ii. IT/Cyber Security Risk Management
  iii. Business Continuity Management, BCP [Business Continuity Plan], DRP [Disaster Recovery Plan] and BIA [Business Impact Assessment]
  iv. IRDAI Cyber Security framework and regulatory measures

v. Cyber Security Standards & Frameworks: RBI, IRDAI, NIST, ISO 27001, ISO 22301, COBIT, PCIDSS, CIS, etc.
vi. OWASP Top 10
vii. End Point Security
viii. Network Security
ix. Information System Audit
x. Vendor Risk Management /TPRM [Third part Risk management]
xi. Next Generation SOC, Artificial Intelligence, Machine Learning

Note:

- The overall scope is indicative in nature. NIA shall have right to provide any clarification in the matter. The interpretation of the NIA would be final and binding on the Bidder.
- The bidder has to use industry standard licensed tools to perform the activities (particularly for VA&PT) mentioned in Scope of Work.
- The bidder has to ensure no adverse impact/denial of service takes place in NIA's Infra & Applications while/subsequent upon carrying out activities in Scope of Work.

12.1 Eligibility Criteria for Team to work on activities mentioned in scope of work

12.1.1 The dedicated team must be with the NIA for the duration of the assignment. The team members for NIA project must have professional qualifications - CISA, CISSP/CEH/ISO 27001:2013 Lead Auditor. (Attested Copy of certificate & detail of team members to be submitted by bidder within one week from issuing of work order)

12.1.2 The bidder must have on rolls at least one Project Manager and one additional member who have similar experience as that of the Project Manager. The team leader should have personally involved in at least one similar assignment as mentioned in scope of work. The Project Manager must have at least 5 Years' experience of the Information/Cyber Security related Audit & Information Security Training Services. (CV of the Employee with signature at the bottom to be submitted by the bidder within one week from issuing of work order).

12.1.3 The selected Bidder firm shall be required to submit satisfactory documentary evidence for carrying out a background check on the personnel deployed at the NIA for this assignment. (Declaration on letter head)

13.0) PROJECT SCHEDULE

12.1.4 The Bidder shall complete the entire activity mentioned in SOW Sec 12.0 (Phase I, II, III, IV & V) within 34 weeks (The timelines for Assurance System audit as per phase -1 of Section 12.0 (A) and Phase III VA&PT report as per Section 12.0 (C) Vulnerability assessment & Penetration Testing should be as per the table given below) excluding the time required by NIA's IT partners to complete actual procurement/installation/up gradation of components.

13.1) The bidder has to perform the comprehensive audit as per IRDAI issued information & cyber security guidelines Ref no. IRDAI/GA&HR/GDL/MISC/ 88/04/2023 released on 24th April'2023 and any other subsequent amendments to these guidelines or any new guideline released on Cyber Security which falls during contract period. Along with this, New India desires to carry out thorough System Audit.

13.2) Aside from this, NIA intends to conduct vulnerability assessment & Penetration Testing for the network devices, security devices, various servers residing at the critical locations like the Data Centre (Rabale, Mumbai), Disaster Recovery site (Bangalore) & Near Disaster Recovery site (Airoli, Mumbai) etc., public facing websites, Critical API's security testing & various other applications to verify the controls in place, Information Security Training for vendors, Employees and Senior Management. The bidder should adhere to the project schedule as stipulated in the table below for Phase I, Phase II, Phase III, Phase IV & Phase V. Failure to do so would lead to Liquidated Damages as stated in this tender, unless New India grant an extension to the bidder in writing for completion of the activities beyond the timelines.

Particulars	Timeline for completion
Phase I (A)	
Assurance audit report	Should be submitted within First Quarter of Upcoming Financial Year. In case the audit starts late due to some unforeseen circumstances, Report must be submitted within 90 Days from start of engagement. (Maximum Duration for Audit and Submission of Report should not exceed 90 days in any case)
Phase II (B)	
System Audit Report	Should be submitted within 90 Days from start of engagement and sharing of CV's of auditors.
Phase III (C)	
1st VA&PT	Reports should be submitted within 8 weeks of engagement (April- May)
Black box testing of internet facing applications	1 Week (June 1st Week)
1st Revalidation testing	8 Weeks (July –August)
2nd VA&PT	8 Weeks (October -November)
Black box testing of internet facing applications	1 Week (November Last week)
2nd Revalidation testing	8 Weeks (January - February)
	34 Weeks

Note- If engagement gets delayed then Engagement month will be considered as start month and whole VAPT is to be completed by February of that FY.	
Phase IV (D)	
Review of existing documents and their status of implementation. Phase 4(a)	10 Weeks
Creation of New Secure Configuration documents and its implementation. Phase 4 (b)	10 Weeks for New document created and its implementation
Creation of New Secure Configuration documents and its implementation above 20 Documents Phase 4 (c)	3 Weeks
Note – Starting date will be as per discretion of NIA	
Phase V (E)	
Sessions will be arranged as per time availability within engagement timeline.	
Total time for whole engagement as per SOW Sec 12.0	**End of February of that particular FY.**

14.0) PAYMENT TERMS

- The payments shall be released as per the table given below. The Company also reserves the right to prescribe additional documents for release of payments and the bidder shall comply with the same.

SN	For each phase other than Section-12.0(C) VA&PT	Payment
1	Post Submission of all deliverable as per Scope of Work mentioned in Section-12.0 (A,B&D,E),acceptance of reports & Sign off from NIA	100%

SN	For phase-3 Section-12.0(C) VA&PT	Payment
1	Post Submission of deliverable (1st VA&PT and 1st Revalidation testing) as per Scope of Work mentioned in Section-12.0(C) acceptance of reports & Sign off from NIA	50%
2	Post Submission of deliverable for (2nd VA&PT and 2nd Revalidation testing) as per Scope of Work mentioned in Section-12.0(C) acceptance of reports & Sign off from NIA	50%

- No Advance Payment will be made in any case.

15.0) PRICE

15.1) The bidders should quote base price. Applicable taxes will be paid as actuals.

15.2) NIA will not pay expenses/ charges/fees/ travelling expenses/ boarding expenses/ lodging expenses/ conveyance expenses/ out of pocket expenses other than the commercial quoted by the bidder for the project related work.

15.3) There shall be no escalation in the prices once the prices are fixed and agreed to by the Company and the bidders. But, any benefit arising out of any subsequent reduction in the prices due to reduction in taxes after the prices are fixed and before the agreement should be passed on to the Purchaser /Company.

16.0) PENALTY TERMS

16.1) The engagement should start within a week from the date of issue of purchase order/work order**.** In case the bidder deviates from time lines provided in the Project Schedule 13.0 or such authorized extension as may be permitted in writing by NIA, NIA shall impose a penalty@ 0.5 % of PO value per week subject to a maximum of 10% of total charges for each phase.

Sr. No.	Category	Timeline for Submission	Penalty
1	Phase-1 & Phase-2	Within 90 days from the start of engagement.	per week 0.5% of total charges for this phase
2	Phase-3	Within 1 week from completion of each activity as desired in 13.0	per week 0.5% of total charges for this phase
3 (a)	Phase-4 (a)	Within 11 Weeks from the start of engagement	per week 0.5% of total charges for this phase
3 (b)	Phase-4 (b)	Within 11 Weeks from the start of engagement	per week 0.5% of total charges for this phase
3 (c)	Phase-4 (c)	Within 4 Weeks from the start of engagement	per week 0.5% of total charges for this phase
4	Executive summary report for Assurance audit as per IRDAI Circular (Please refer 13.2 on pg no.10)	Within First Quarter of Current Financial Year (April to June) or if engagement is delayed within 90 Days of start of engagement	per week 0.5% of total charges for this phase

17.0) PERFORMANCE BANKGUARANTEE:

17.1) The selected bidder would be required to submit a Performance Bank Guarantee to the Company for an amount equivalent to 3% of Contract value within 30 days of purchase order issue date. The performance guarantee would be for the entire period of the Contract. If the Performance guarantee is not submitted, the NIA reserves the right to cancel the contract. The Performance Guarantee would be returned to the Service provider on expiry or termination of the contract and after the claim period of 3 months.

17.2) The Bank Guarantee should be issued by any nationalized/scheduled Bank with a validity of Contract Period.

17.3) Performance Guarantee may be forfeited in the event of a breach of contract by the bidder solely due to the reasons attributable to the bidder.

18.0) GENERAL TERMS

18.1) The agreement shall be in force for a period of 1 year. The successful bidder will enter into contract for a period of 1 year from the date of Purchase Order. NIA reserves right to extend the contract by another year upon the satisfactory performance of the vendor on the same terms and conditions.

18.2) The successful bidder is required to sign NDA as per Annexure-7 with NIA to maintain and protect the confidentiality of Data.

18.3) At any time prior to the last date of receipt of bids, the Company may, for any reason, whether at its own initiative or in response to clarifications requested by the prospective bidders, modify the tender document by clarifications. The Clarifications, if any, issued by the Company at any time before the due date of submission of the bid will become part of the tender document and would be notified on the official web-site of NIA as well as at E-Procurement portal. Vendors are requested to regularly check the Company Website (https://newindia.co.in) as well as on e-Procurement portal (**https://tenderwizard.com/NIAEPROC**) for addendum/corrigendum, if any till the closing date of the tender.

18.4) If the bidder wishes to depart from any terms and conditions of the tender in any respect he shall draw the attention to such points of departure explaining fully the reason as thereof and furnish separately adopting the form given Annexure– 5. Unless this is done, the requirements of the tender will be deemed to have been accepted in every respect. The Company reserves the right to accept/reject any or all of the deviations submitted by the bidder

18.5) The queries may be communicated only through e-mail on email ID: rfpnw.itho@newindia.co.in and response to query will be by return e-mail. No queries will be accepted on telephone or through any means other than e-mail. The queries should be sent in .xls/.xlsx format only as per format provided in Annexure-5 only. No other format shall be accepted.

SECTION II

PART A – TECHNICAL BID (ONLINE)

The technical bid, apart from the all online template filling up, should contain the **scanned copies of all requisite documentary proofs** related to the Eligibility Criteria along with the following documents. The documents shall be arranged in the same order as mentioned in online bidding format.

a) Demand Draft/ Bankers' Cheque for Tender Document Fees.
b) Bank Guarantee for EMD.
c) Proposal covering methodology, approach & timelines
d) Power of attorney/authorization letter
e) Eligibility Criteria as per Annexure-1
f) Bidder profile as per Annexure-2

PART A – TECHNICAL BID (OFFLINE)

The following documents are required to be submitted offline in physical/hard copies to The Chief Information Security Officer (CISO) R. Sheshadri, Fifth Floor,The New India Assurance Co. Ltd., Head Office,87, M G Road, Fort, Mumbai-400001 by 3:30 PM, 27/05/2024 in one sealed envelope super-scribed as "Offline Document Submission for **"e-Tender for Selection of Vendor for Verification of Regulatory Compliance,System Audit, VA&PT, SCD and Info-Security Training (TENDER NO: NIA/HO/IS/05-2024/01)"** failing which the bidder may be disqualified and their tender may not be opened:

a) Original DD/Bankers Cheque towards tender document Fees.
b) Original Bank Guarantee towards EMD amount.

The details of the DD/any other accepted instrument, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time. Otherwise the submitted bid will not be acceptable.

PART B- COMMERCIAL BID (ONLINE)

a) Commercial bid as per Annexure-3

Note: No offline documents are required to be submitted for commercial bid.

SECTION III

GENERAL TERMS & CONDITIONS

1.0) PROCEDURE FOR PROCESSING THE TENDER DOCUMENT:

1.1) The Committee constituted by the Company will open the Cover 'A' electronically and off-line document cover physically. In case the cover 'A' does not contain Pay Order/Demand Draft/Bank Guarantee towards Earnest Money Deposit and tender document fees, their offer would be rejected.

1.2) Each and every aspect in the Eligibility Criteria and Technical Bid including deviations, if any, would be discussed by the Committee.

1.3) The commercial Bids of technically qualified bidders will be opened by the Committee electronically in the presence of the bidders who wish to be present for opening. L1 will be identified on the total Price of the Commercial Bid Summary.

1.4) Any commercial bid incomplete in any respect will be disqualified.

1.5) This procedure is subject to changes, if any, and the procedure adopted by the Company for opening the tender shall be final and binding on all the parties.

2.0) TECHNICAL EVALUATION

2.1) Only those Bidders and Bids who have been found to be in conformity with the terms and Conditions of Eligibility Criteria would be considered by the Company for further proceedings.

2.2) The Company will evaluate the technical bid for each and every line item for its conformity with the specifications as stated in the RFP.

2.3) During evaluation and comparison of bids, the Company may, at its discretion ask the bidders for clarification of its bid. The request for clarification shall be either through email or a query through e-Procurement portal and no change in prices or substance of the bid shall be sought, offered or permitted. No post bid clarification/suggestions at the initiative of the bidder shall be entertained.

3.0) PRICE (COMMERCIAL) BID EVALUATION

3.1) Only those Bidders who qualify in Eligibility Criteria Evaluation and Technical evaluation would be shortlisted for commercial evaluation. The commercial Bids of technically qualified bidders will be opened by the Committee electronically. L1 will be identified on the total Price of the Commercial Bid Summary.

4.0) AGREEMENT

The successful bidder shall enter into a detailed Agreement with NIA. A Performa/draft Agreement as mentioned in Annexure-6. However, the Company reserves the right to alter/vary/amend/modify all or any of the terms set out in the said Performa/draft Agreement. The successful bidder shall sign and return the contract (Annexure-6) within 4 weeks from the date of Purchase Order from NIA.

Encl :

Annexure-1 (Eligibility Criteria for bidders)
Annexure-2 (Bidder's Profile)
Annexure-3 (Commercial Bids)
Annexure-4 (Queries)
Annexure-5 (Deviations)
Annexure-6 (Agreement Draft)
Annexure-7 (Non-Disclosure Agreement)
Annexure-8 (Special Instructions to Bidders for E-Tendering)

ANNEXURE-1
ELIGIBILITY CRITERIA

S.N.	Eligibility Criteria	Documents Required
Eligibility Criteria for Bidder		
1	The bidder should be a public / private limited company registered in India and should have been in existence for a minimum period of **FIVE** years.	Certificate of Incorporation
2	The Bidder should have a minimum turnover of Rs.10 crores per annum for each of the following financial years (2020-21, 2021-22, 2022-23).	Audited Financial statements / balance sheet /CA Certificate for the respective financial years.
3	The Bidder should have a positive net worth in each of the following financial years (2020-21, 2021-22, 2022-23).	
4	The bidder should be empaneled by CERT -In as Information/Cyber Security Organization for the period valid up to Dec 31, 2023.	Certificate of Empanelment with CERT –In
5	The bidder should have conducted System Audit for minimum 2 PSU/ State/ Central government organizations in last 5 years. Out of the 2, atleast 1 should be from the BFSI domain in last 5 years	Purchase Order / Engagement Letter / Agreement signed between the parties.
6	The bidder should have conducted VA&PT for minimum 2 PSU/ State/ Central government organizations. Out of the 2,atlleast 1 should be from the BFSI domain in last 5 years	Purchase Order / Engagement Letter / Agreement signed between the parties.
7	The Bidder must have at least 3 CISA& 3 CISSP/ISO 27001: 2013/22 Lead Auditors/CEH Certified Professionals as employees.	Name of the Employee & Copy of certificates
8	The bidder must have never been blacklisted/barred/disqualified by any regulator/statutory body.	Self Declaration
9	The bidder should not be involved in NIA's IT audit Projects from last 1 year from the tender publishing date.	Self-Declaration by Vendor
10	Bidder should be the prime bidder and no consortium is allowed for the in-scope services to be offered.	A self-certified letter in this regard to be provided.

11	The bidder should have handled at least 5 assignments/ Services related to cyber security trainings/ awareness sessions and content development to BFSI institutions in India during last three financial years [i.e.2023-24, 2022-23, 2021-22].	Purchase Order / Engagement Letter / Agreement signed between the parties.
12	The bidder should have experience in handling training in at least **5** of the following areas: Introduction to Cyber Security, IT/ Cyber Risk Management, Case Studies on Recent Cyber Security Breaches, Case Studies on Cyber Laws, Cyber Security Framework, Data Protection and Privacy, Vulnerability Management, Encryption and Cryptography, Third-Party Risk Management, Security Auditing, Network Security, Endpoint Security, Web Application Security, Threat Hunting and Intelligence, Wireless Security, Physical Security, ISO Certification, Business Continuity Management, Cyber Security – Regulatory Measures, Cyber Fraud Investigation, Cyber Security Governance, Master Directions and advisories issued by the regulator, Insurance Domain covering Frauds in Insurance LOB's.	Purchase Order / Engagement Letter / Agreement signed between the parties/ Training evidence with customer sign-off

ANNEXURE – 2
Bidder's Profile

Sr. No.	Details	Remarks
1	Name & Address of the Bidder	
2	PAN No. (Attach copy)	
3	Correspondence address at Mumbai with contact person/s name/s, telephone number, mobile number etc.	
4	Name and designation of the person authorized to sign the Bid / proposal and all other documents incidental to the tender.	
5	Contact person/s name/s, telephone number, mobile number etc. and escalation matrix for the purpose of this tender	

ANNEXURE- 3

COMMERCIAL BID

Sr. No	Phase	Price in INR
1	Phase I	
2	Phase II	
3	Phase III	
4 (a)	Phase IV (a)	
4 (b)	Phase IV (b)	
4 (c)	Phase IV (c) per document/implementation cost	
5	Information Security Training	
	Total (A)	

1) L1 will be identified on the Grand Total (A) of the Commercial Bid summary.
2) The price should be as per Section I, Sr no 15.0

ANNEXURE-4

QUERIES-FORMAT

Sr No	Bidder Name	Page No(tender Ref)	Clause(tender Ref)	Description in the tender (tender Ref)	Query
1					
2					

Note : The queries may be communicated only through e-mail and response to query will be by return e-mail. No queries will be accepted on telephone or through any means other than e-mail. The queries should be send in .xls/.xlsx format with above fields only.

ANNEXURE-5

FORMAT- DEVIATIONS

Sr. No	Bidder Name	Page No(tender Ref)	Clause(tender Ref)	Description in the tender (tender Ref)	Deviation Details	Reasons for deviation
1						
2						

Note: NIA reserves the right to accept/reject any or all of the deviations shown by the bidder.

ANNEXURE – 6

AGREEMENT DRAFT
(Should be on Rs.100/-stamp paper)

This agreement made on this_____day of_____between_____hereinafter called the "BIDDER" and THE NEW INDIA ASSURANCE CO. LTD., hereinafter called "THE COMPANY" sets forth the terms and conditions for the selection of vendor for verification of Regulatory Compliance, System Audit & VA&PT.

1.0) SCOPE OF WORK(SOW)

Phase-1

A) Assurance Audit of NIA's IT Infrastructure as per IRDAI framework on Information & Cyber Security

As per IRDAI guidelines & industry standards on information and cyber security for insurers, the bidder has to perform following activities:

- Comprehensive Assurance audit of NIA for Information Security/Cyber Security and according to Information and Cyber Security Guidelines V 1.0 Ref no. IRDAI/GA&HR/GDL/MISC/88/04/2023 released on 24th April'2023 (all the domains of circular have to be covered) and any other subsequent amendments to these guidelines or any new guideline released on Cyber Security which falls during contract period. Auditor also has to follow amendments done in VAPT guidelines issued on 30-12-2020 Ref. NO.: IRDA/IT/CIR/MISC/301/12/2020.
- Audit will include scope and compliance as per above mentioned circular.
- The auditor has to refer IRDAI Audit Checklist of total 348 controls shared with the guidelines for audit.
- Review of preparedness/readiness of the NIA vis-à-vis IRDAI Circular on Cyber Security Framework.
- Auditor should be fulfilling eligibility criteria mentioned in Annexure IV of the IRDAI guidelines.
- Audit of the NIA's Current Cyber Security Architecture.
- The bidder has to provide recommendations to increase the effectiveness of the security controls.
- Knowledge Transfer during execution of the Assignment, provide documentation and material.
- The bidder would recommend improvements to better align the security architecture with business objectives, the NIA's information& cyber security policy and industry best practices.

Deliverables

- NIA would need separate comprehensive reports on all the aspects covered in the aforementioned scope of work.
- The report has to be formulated Category wise as defined in IRDAI document. It should incorporate methodology used, gaps identified, severity of gaps, possible issues that can occur, various risks which may arise, mitigation methods etc.
- Auditor has to share the report in format shared by IRDAI i.e Annexure III.
- Auditor has to provide Certificate on Cyber security controls as per Annexure-5 of Information and Cyber Security Guidelines v 1.0 Ref no. IRDAI/GA&HR/GDL/MISC/ 88/04/2023 released on 24th April'2023. The detailed report of review should be as per Annexure A of Annexure -5 of the same guideline.
- Graphical representation outlining the as-is [current state] Enterprise information/cyber Security Architecture.
- Graphical representation outlining the to-be [future state] Enterprise information/cyber Security Architecture.
- The summary of cyber security readiness exercise and recommendations for improvement areas.
- A roadmap which includes prioritization of improvement areas.

Phase-2

B) System Audit

As part of this scope, the bidder has to perform comprehensive system audit for the following sections where process walkthroughs have to be done to understand the processes in place, risk areas have to be identified, design & operating effectiveness of the controls in place have to be evaluated, control gaps if any have to be identified and has to provide recommendations for improvement areas.

It will include 25-30 applications, no of IP's (around 280-300) that includes network devices, security devices, different servers, databases etc), approx. 20 API's workflow security review. The scope will involve Third Party Administrator (TPA) risk assessment audit remotely which are approximately 16 in number, On-call and On-premise Vendor Risk assessment for vendors providing services remotely to NIA (For On-Premise the number of vendors sites outside Mumbai are approximately 3 in number in regions - Noida, Bangalore, Kolkata).

The vendor has to submit a checklist for system audit domain covering all the parameters and following best cyber security practices, guidelines from ISO, IRDAI, RBI, NIST, SOC, Data Privacy etc.

The parameters for System Audit is mentioned below.

- IT Governance & Strategy
- High level system architecture review
- Information & Cyber Security policy & Procedures
- Assessment of in-scope business applications
- Data Center(DC), Disaster Recovery (DR) & NDR (Near Disaster Recovery) operations
- SDLC Audit
- Change Management

- Patch Management
- Access Management
- Asset Management
- IT Operations (Configuration management, Job scheduling, Backup & Restore etc)
- Data Security
- Network security
- Email Security
- Endpoint Security
- System Acquisition, Development & Maintenance
- Incident Management
- Database Security
- Mobile &Tele working Security
- Physical & Environmental Security
- Antivirus Controls
- TPA (Third Party Admin1strator) Risk Assessment (16)
- Vendor Risk Assessment
- Cryptography & Key management
- Virtualization
- Cloud Security
- Security Logging & Monitoring
- Audit Trails
- Data Privacy

Deliverables:

- NIA would need a comprehensive report on all the aspects for aforementioned areas.
- Network architecture review will involve planning, review of all deployments and NIA needs a Comprehensive report on how to improve and Consolidate Various Network Architectures.
- The report has to be formulated Category wise as per areas mentioned hereinabove. It should incorporate methodology used, gaps identified, possible issues that can occur, various risks which may arise, mitigation methods etc.
- Vendor Risk Assessment and TPA risk assessment reports should be a separate report from System audit report and will be per vendor.

Phase-3

C) Vulnerability Assessment& Penetration Testing

1) To check the robustness of the IT infrastructure, applications & identify vulnerabilities, the bidder has to perform vulnerability assessment and penetration testing (through grey box testing).

Grey Box Testing

1) It will include number of IPs (around 280-300), 25 API's and about 30 applications for the vulnerability assessment & penetration testing.
2) As per guidelines issued on 29-12-2020 Ref. NO.: IRDA/IT/CIR/MISC/301/12/2020 by IRDA the bidder has to perform Vulnerability assessment and penetration testing (through grey box testing) annually for Intranet applications (approx. 12-16) and once in 6 months for internet facing applications (approx. 12-14).

3) Every VA&PT testing will involve 2 cycles one at the beginning of VA&PT for identification of gaps and to check for known vulnerabilities, and a retesting post closure of vulnerabilities identified (Revalidation testing).

    i. 1st VA&PT for identification of gaps will include IP's about 280-300 in number, 25 API's and about 30 applications.
    ii. 2nd VA&PT for identification of gaps will include 12-14 internet facing application and Wireless controller & access points.

4) Revalidation Testing

    i. 1st Revalidation testing will be done for internet facing applications (approx. 12-14), 25 API's and Wireless controllers for access point after submitting initial report of 1st VA&PT Grey box testing for identification of gaps.
    ii. 2nd Revalidation testing will include all the 30 application, and IP's around 280-300 after the report of 2nd VA&PT Grey box testing for identification of gaps.

6) Timelines for completing 1st VA&PT Testing for identification of gaps and 1st Revalidation testing should be within 4 months and timeline for completing 2nd VA&PT Testing for identification of gaps and 2nd Revalidation testing should be within 4 months.

Black Box Testing

1) For closure of identified gaps in all internet facing applications and Infrastructure components, External Black Box Penetration Testing should be done within one month after receiving the 1st and 2nd VA&PT report for identification of gaps.

VA&PT should be comprehensive that includes following activities:

- Network Scanning/Surveying
- Port Scanning
- Port sweep
- System & OS Fingerprinting
- System Identification & Trusted System Scanning

- Vulnerability Scanning
- Service Fingerprinting
- Secure Configuration Review

Website/application assessment should be done against all known vulnerabilities Including but not limited to latest OWASP vulnerabilities:

- SQL injection
- Broken Authentication and Session Management
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security Mis-configuration
- Insecure Cryptographic storage
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-Validated Redirects and Forwards
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Any other loopholes, which makes websites & applications vulnerable to malicious attacks.

API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities:

- Broken Object level authorization
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted resources consumption
- Broken function level authorization
- Unrestricted access to sensitive business flows
- Server side request forgery
- Security misconfiguration
- Improper inventory management
- Unsafe consumption of API's

Deliverables:

- NIA would need a comprehensive report on all the aspects covered in the scope of work with detailed recommendations to plug the vulnerabilities.
- It should incorporate methodology used, gaps identified, possible issues that can occur, possible risks which may arise, mitigation methods etc.

- In case New deployments of API and Application is done the vendor has to perform VAPT at no additional cost to NIA.

Phase-4

D) Review and Creation of the hardening documents

Phase-4 (a)
The bidder has to review NIA's existing Secure Configuration Documents adopting best practices for server's OS, Database, Security Devices, Network Devices etc. & update the same in case of any gap.

Phase-4 (b) Also Bidder has to scan the whole environment and create new secure configuration documents if any for Windows OS for end devices, Server's OS, Database, security devices, Network devices etc. and see through its implementation with the existing vendor. As per existing requirement Vendor has to create and implement 20 Documents. The cost mentioned for this phase is a Onetime requirement and if contact is extended by 1 more Year this cost will not be Considered.

Phase-4 (c) The vendor also has to quote a base price per document for the requirement over and above as mentioned in Phase -4 (b) i.e if count exceeds 20 Documents.

Deliverables:

- NIA would need a comprehensive report on aforementioned aspects covered in the scope of work.
- It should incorporate methodology used, gaps identified, possible issues that can occur, possible risks which may arise, mitigation methods etc.
- The Vendor have to submit the Implementation report evidence for the new configuration document with all the details, e. (Plan, Use Case for NIA, Implementation checklist suggested and implemented).

Phase-5

E) Information Security Training to Employees, Vendors and Senior Management

- As part of the tender the Vendor has to provide Information Security Training to Employees and 4 Sessions will be arranged Annually where each session will cover 1 Region (North, South, East, West).
- Training to Vendor will be arranged on an annual basis. (1 Session in a Year)
- Senior Management training will be arranged twice a Year covering new

threat vectors, Cyber security Hygiene etc.

- Training to NIA IT team and IS team.

Deliverables:

- The training shall be conducted both in offline and Online/Virtual mode as per NIA requirement.
- The content format for conducting Information/ Cyber Security Awareness Training program shall include the following:
  i. E-Mail content, Multimedia [Animations and transitions]
  ii. SMS Content
  iii. Web Content
  iv. Quizzes
  v. Manual/Booklets/Brochures
  vi. Publishing Screen Savers across the NIA's End User Workstations from Cyber Security perspective.
  viii. Cyber Security Awareness Sessions /Presentations [PPT]

- **Indicative list of Information/Cyber Security Awareness topics for Vendor and NIA IT and IS team :**
  i. Cyber Security Basic Principles covering CS Basic terminologies, different frameworks and Security Governance.
  ii. Cyber Security as an enterprise-wide risk management issue covering Role of Business Heads in Cyber Security and the need of cyber security posture/preventive, detective, corrective controls
  iii. IT Risk management covering different types of Risks, key metrics, reporting structure and Risks mitigation measures.
  iv. Business Continuity Management [covering BIA, BCP and DRP etc.,]
  v. Cyber Security Framework [NIST, COBIT etc.,]
  vi. Current Trends and Techniques in Cyber Security environment
  vii. IT/Cyber Security Risk Management
  viii. Vendor Risk Management/ TPRM [Third Party Risk Management]
  ix. Social Engineering attacks
  x. Cyber Security Risks in Remote Working
  xi. Cloud Computing Security and challenges
  xii. Importance of Information Security / Cyber Security Policies, Guidelines
  xiii. Threat Intelligence Advisories like US-CERT, CSITE, CERT-In, Meity etc.,
  xiv. IT Act 2000, 2008 IT Act amendment, Data Protection Bill (DPDP Act)
  xv. Any other latest topic/happenings related to cyber security

- **Indicative list of Information/Cyber Security Awareness topics for Vendor and NIA IT and IS team :**
  i. Introduction to Cyber Security
  ii. Basic Cyber Security Terminology
  iii. Business Continuity Management
  iv. Incident Detection and Response
  v. Recent Cyber Security Breaches
  vi. Digital Payments and Security measures
  vii. Importance of Information Security / Cyber Security Policies, Guidelines
  viii. Any other latest topic/happenings related to cyber security
  ix. Latest topics related to IT/technology
  x. Hands-on sessions on above topics as per NIA's requirements

- **Indicative list of Information/Cyber Security Awareness topics for Vendor and NIA IT and IS team :**
  i. Basic Cyber Security Terminology
  ii. IT/Cyber Security Risk Management
  iii. Business Continuity Management, BCP [Business Continuity Plan], DRP [Disaster Recovery Plan] and BIA [Business Impact Assessment]
  iv. IRDAI Cyber Security framework and regulatory measures
  v. Cyber Security Standards & Frameworks: RBI, IRDAI, NIST, ISO 27001, ISO 22301, COBIT, PCIDSS, CIS, etc.
  vi. OWASP Top 10
  vii. End Point Security
  viii. Network Security
  ix. Information System Audit
  x. Vendor Risk Management /TPRM [Third part Risk management]
  xi. Next Generation SOC, Artificial Intelligence, Machine Learning

Note:

- The overall scope is indicative in nature. NIA shall have right to provide any clarification in the matter. The interpretation of the NIA would be final and binding on the Bidder.
- The bidder has to use industry standard licensed tools to perform the activities (particularly for VA&PT) mentioned in Scope of Work.
- The bidder has to ensure no adverse impact/denial of service takes place in NIA's Infra & Applications while/subsequent upon carrying out activities in Scope of Work.

1.1) Eligibility Criteria for Team to work on activities mentioned in scope of work

1.1.1) The dedicated team must be with the NIA for the duration of the assignment. The team members for NIA project must have professional qualifications - CISA, CISSP/CEH/ISO 27001:2013 Lead Auditor. (Attested Copy of certificate & detail of team members to be submitted by bidder within one week from issuing of work order)

1.1.2) The bidder must have on rolls at least one Project Manager and one additional member who have similar experience as that of the Project Manager. The team leader should have personally involved in at least one similar assignment as mentioned in scope of work. The Project Manager must have at least 5 Years' experience of the Information/Cyber Security related Audit & Information Security Training Services. (CV of the Employee with signature at the bottom to be submitted by the bidder within one week from issuing of work order).

1.1.3) The selected Bidder firm shall be required to submit satisfactory documentary evidence for carrying out a background check on the personnel deployed at the NIA for this assignment. (Declaration on letter head)

2.0 PROJECT SCHEDULE

2.1) The Bidder shall complete the entire activity mentioned in SOW Sec 12.0 (Phase I, II, III, IV & V) within 34 weeks (The timelines for Assurance System audit as per phase -1 of Section 12.0 (A) and Phase III VA&PT report as per Section 12.0 (C) Vulnerability assessment & Penetration Testing should be as per the table given below) excluding the time required by NIA's IT partners to complete actual procurement/installation/up gradation of components.

2.2) The bidder has to perform the comprehensive audit as per IRDAI issued information & cyber security guidelines Ref no. IRDAI/GA&HR/GDL/MISC/ 88/04/2023 released on 24th April'2023 and any other subsequent amendments to these guidelines or any new guideline released on Cyber Security which falls during contract period. Along with this, New India desires to carry out thorough System Audit.

2.3) Aside from this NIA intends to conduct vulnerability assessment & Penetration Testing for the network devices, security devices, various servers residing at the critical locations like the Data Centre (Rabale, Mumbai) ,Disaster Recovery site (Bangalore) & Near Disaster Recovery site (Airoli, Mumbai) etc., public facing websites, Critical API's security testing & various other applications to verify the controls in place, Information Security Training for vendors, Employees and Senior Management. The bidder should adhere to the project schedule as stipulated in the table below for Phase I, Phase II, Phase III, Phase IV & Phase V. Failure to do so would lead to Liquidated Damages as stated in this tender, unless New India grant an extension to the bidder in writing for completion of the activities beyond the timelines.

Particulars	Timeline for completion
Phase I (A)	
Assurance audit report	Should be submitted within First Quarter of Upcoming Financial Year. In case the audit starts late due to some unforeseen circumstances, Report must be submitted within 90 Days from start of engagement. (Maximum Duration for Audit and Submission of Report should not exceed 90 days in any case)
Phase II (B)	
System Audit Report	Should be submitted within 90 Days from start of engagement and sharing of CV's of auditors.
Phase III (C)	
1st VA&PT	Reports should be submitted within 8 weeks of engagement (April- May)
Black box testing of internet facing applications	1 Week (June 1st Week)
1st Revalidation testing	8 Weeks (July –August)
2nd VA&PT	8 Weeks (October -November)
Black box testing of internet facing applications	1 Week (November Last week)
2nd Revalidation testing	8 Weeks (January - February)
	34 Weeks
Note- If engagement gets delayed then Engagement month will be considered as start month and whole VAPT is to be completed by February of that FY.	
Phase IV (D)	
Review of existing documents and their status of implementation. Phase 4(a)	10 Weeks
Creation of New Secure Configuration documents and its implementation. Phase 4 (b)	10 Weeks for New document created and its implementation
Creation of New Secure Configuration documents and its implementation above 20 Documents Phase 4 (c)	3 Weeks
Note – Starting date will be as per discretion of NIA	
Phase V (E)	
Sessions will be arranged as per time availability within engagement timeline.	
Total time for whole engagement as per SOW Sec 12.0	**End of February of that particular FY.**

3.0) PAYMENT TERMS

- The payments shall be released as per the table given below. The Company also reserves the right to prescribe additional documents for release of payments and the bidder shall comply with the same.

SN	For each phase other than Section-1.0 C) VA&PT	Payment
1	Post Submission of all deliverable as per Scope of Work mentioned in Section-1.0(A,B,D & E),acceptance of reports & Sign off from NIA	100%

SN	For phase-3 Section-1.0(C) VA&PT	Payment
1	Post Submission of deliverable (1st VA&PT and 1st Revalidation testing) as per Scope of Work mentioned in Section-1.0(C),acceptance of reports & Sign off from NIA	50%
2	Post Submission of deliverable for (2nd VA&PT and 2nd Revalidation testing) as per Scope of Work mentioned in Section-1.0(C) acceptance of reports & Sign off from NIA	50%

- No Advance Payment will be made in any case.

4.0) PRICE

4.1) The bidders should quote base price. Applicable taxes will be paid as actuals.

4.2) NIA will not pay expenses/charges/fees/travelling expenses/boarding expenses/ lodging expenses/conveyance expenses/out of pocket expenses other than the commercial quoted by the bidder for the project related work.

4.3) There shall be no escalation in the prices once the prices are fixed and agreed to by the Company and the bidders. But, any benefit arising out of any subsequent reduction in the prices due to reduction in taxes after the prices are fixed and before the agreement should be passed on to the Purchaser /Company.

5.0) PENALTY TERMS

5.1) The Engagement has to be started within a week from the date of issue of purchase order. In case the bidder deviates from time lines provided in the Project Schedule (Section 2.0) or such authorized extension as may be permitted in writing by NIA, NIA shall impose a penalty@ 0.5 % of PO value per week subject to a maximum of 10% of total charges for each phase.

Sr. No.	Category	Timeline for Submission	Penalty
1	Phase-1 & Phase-2	Within 90 days from the start of engagement.	per week 0.5% of total charges for this phase
2	Phase-3	Within 1 week from completion of each activity as desired in Section 2.0	per week 0.5% of total charges for this phase
3 (a)	Phase-4 (a)	Within 11 Weeks from the start of engagement	per week 0.5% of total charges for this phase
3 (b)	Phase-4 (b)	Within 11 Weeks from the start of engagement	per week 0.5% of total charges for this phase
3 (c)	Phase-4 (c)	Within 4 Weeks from the start of engagement	per week 0.5% of total charges for this phase
4	Executive summary report for Assurance audit as per IRDAI Circular (Pls refer 2.2 on pg no.10)	Within First Quarter of Current Financial Year (April to June) or if engagement is delayed within 90 Days of start of engagement	per week 0.5% of total charges for this phase

6.0) PERFORMANCE BANK GUARANTEE:

6.1 The selected bidder would be required to submit a Performance Bank Guarantee to the Company for an amount equivalent to 3% of Contract value within 30 days of purchase order issue date. The performance guarantee would be for the entire period of the Contract. If the Performance guarantee is not submitted, the NIA reserves the right to cancel the contract. The Performance Guarantee would be returned to the Service Provider on expiry or termination of the contract and after the claim period of 3 months.

6.2 The Bank Guarantee should be issued by any nationalized/scheduled Bank with a validity of Contract Period.

6.3 Performance Guarantee may be forfeited in the event of a breach of contract by the bidder solely due to the reasons attributable to the bidder.

7.0) GENERAL TERMS

7.1 The agreement shall be in force for a period of 1 year. The successful bidder will enter into contract for a period for 1 year from the date of Purchase Order. NIA reserves right to extend the contract by another year upon the satisfactory performance of the vendor on the same terms & conditions.

7.2 The successful bidder may be required to sign NDA as per Annexure-8 with NIA to maintain and protect the confidentiality of Data.

8.0) ROYALTIES AND PATENTS

Any royalties or patents or the charges for the use or infringement thereof that may be involved in the contract shall be included in the price. The bidders shall protect the Company against any claims thereof.

9.0) RISK AND TITLE

The risk, title and ownership of the products shall be transferred to the customer upon dispatch of such products to the customer.

10.0) SAVINGS CLAUSE

The bidder's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent the bidder's non-performance is caused by Company's omission to act, delay, wrongful action, failure to provide Inputs, or failure to perform its obligations under this Agreement.

11.0) LIMITATION OF LIABILITY

The bidder represents and warrants that the repair and maintenance of services/products hereby sold do not violate or infringe upon any patent, copyright, trade secret or other property right of any other person or other entity. The bidder agrees that it will and hereby does, indemnify the company from any claim, directly or indirectly resulting from or arising out of any breach or claimed breach of this warranty. Subject to the above and notwithstanding anything to the contrary elsewhere contained herein, the maximum aggregate liability of Bidder for all claims under or in relation to this Agreement, shall be, regardless of the form of claim(s), shall be limited to 100% of contract value.

12.0) LIQUIDATED DAMAGES

If the bidder fails to deliver the services within the time lines specified in the contract, NIA shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 0.5% of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the contract price. Once the maximum is reached, NIA may consider termination of the contract.

Performance of services shall be within the norms specified in the Scope of work (SoW) forming a part of the contract. In case bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the tender.

13.0) DEEMEDACCEPTANCE

Any Deliverable(s) / Work Product(s)/installation & commissioning provided to the Customer shall be deemed to have been accepted if the customer puts such Deliverable(s)/ Work Product(s) /installation & commissioning to use in its business or does not communicate its disapproval of such Deliverable(s) / Work Product(s) /installation & commissioning together with reasons for such disapproval within 30

days from the date of receipt of such Deliverable(s) / Work Product(s) /installation & commissioning.

14.0) INDEMNITY

The Service Provider (SP) shall indemnify, protect and save NIA and hold NIA harmless from and against all claims, losses, costs, damages, expenses, action suits and

other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from (i) an act of gross negligence and willful misconduct of the SP, its employees, its agents, in the performance of the services provided by this contract, (ii) infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components used to facilitate and to fulfill the scope of the site requirement. provided however, (i) NIA notifies the SP in writing immediately on aware of such claim, (ii) the SP has sole control of defense and all related settlement negotiations, (iii) NIA provides the SP with the ass1stance, information and authority reasonably necessary to perform the above, and (iv) NIA does not make any statement or comments or representations about the claim without prior written consent of the SP, except under due process of law or order of the court. It is clarified that the SP shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to NIA's (and/or its customers, users and service providers) rights, interest and reputation.

The SP's should indemnify NIA (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

2.3)1.1. Non-compliance of the SP with laws/government requirements

2.3)1.2. IP infringement

2.3)1.3. Gross negligence and willful misconduct of the SP, its employees and agents

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by NIA arising out of claims made by its customers and/or regulatory authorities.

The SP shall not indemnify NIA for-

(i) Any loss of profits, revenue, contracts, or anticipated savings or
(ii) Any consequential or indirect loss or damage however caused

15.0) JURISDICTION &ARBITRATION

All disputes/differences of any kind whatsoever arising out of or relating to the construction, meaning, operation, effect or breach of the Agreement, then either party may refer to a sole arbitrator who shall be jointly appointed by both the parties or, in the event that the parties are unable to agree on the person to act as the sole arbitrator within 30 days after any party has claimed for arbitration in written form, by three arbitrators, one to be appointed by each party with power to the two arbitrators so appointed, to appoint a third arbitrator within a period of 30days from the appointment of the second of the Arbitrators. The arbitration shall be conducted under the Arbitration &

Conciliation (Amendment) Act, 2015 as amended or re-enacted from time to time. The governing law for the arbitration shall be Indian Law. The proceeding of arbitration shall be conducted in the English language. The arbitration shall be held in Mumbai, India.

16.0) FORCE MAJEURE

The bidder shall not be liable for any delay or failure of performance of any of its obligations under or arising out of this contract, if the failure or delay results from Act of God, refusal of permissions or other Government Act, fire, explosion, accident and the like which renders it impossible or impracticable for the bidder to fulfill its obligations under the contract or any other cause or circumstances of whatsoever nature beyond bidder's control.

17.0) CONFIDENTIALITY

Both parties acknowledge that all materials and information which has or will come in its possession or knowledge in connection with the performance of this agreement, hereof, cons1sts of confidential and proprietary data, whose disclosure to or use by third parties will be damaging or cause loss to the company. The parties agree to hold such material and information in strictest confidence not to make use thereof other than for the performance of this agreement, to release it only to employees requiring such information, and not to release or disclose it to any other parties. The parties shall take appropriateactionwithrespecttoitsemployeestoensurethattheobligationsofnon-use and non-disclosure of confidential information as per NDA is fully satisfied.

18.0) CONFLICT OF INTEREST

The Bidder shall disclose to NIA in writing, all actual and potential conflicts of interest that ex1st, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

19.0) NIA's RIGHT OF INSPECTION AND PERIODIC AUDIT

- Both NIA reserves the right to inspect and monitor/assess the progress of the Service(s) at any time during the course of the Contract. NIA may demand and upon such demand being made, NIA shall be provided with any document, data, material or any other information, which it may require, to enable it to assess the progress of the Service(s).
- NIA shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by the Bidder of its obligations/functions in accordance with the standards committed to or required by NIA and the Bidder undertakes to cooperate with and provide to NIA any other agency appointed by NIA, all documents and other details as may be required by them for this

purpose. Any deviations or contravention identified as a result of such audit/assessment would need to be rectified by the Bidder failing which NIA may, without prejudice to any other rights that it may have, issue a notice of default.

20.0) INFORMATION SECURITY

- The Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, storage tapes or any other media out of NIA's premise without written approval from NIA.
- The Bidder personnel shall follow NIA's information & Cyber security policy and instructions in this behalf.
- Bidder shall, upon termination of this Contract for any reason, or upon demand by NIA, whichever is earliest, return any and all information provided to Bidder by NIA , including any copies or reproductions, both hardcopy and electronic copy.

21.0) NO ASSIGNMENT

The Contract cannot be transferred or assigned by the Bidder without the prior written approval of NIA.

22.0) NON HIRE

Customer acknowledges that personnel to be provided by bidder represent a significant investment in recruitment and training, the loss of which would be detrimental to bidder's business. In consideration of the foregoing, Customer agrees that for the term of this Agreement and for a period of one year thereafter, Customer will not directly or indirectly, recruit, hire, employ, engage, or discuss employment with any bidder employee, or induce any such individual to leave the employ of bidder. For purposes of this clause, a bidder employee means any employee or person who has who has been involved in providing services under this Agreement.

23.0) TERMINATION

Either party shall have the right to terminate this contract / agreement at any time by giving 3 months advance notice in the event that the other party commits a material breach of the agreement and fails to make good such default to the non-defaulting party's reasonable satisfaction within thirty (30)days. In the event of termination NIA shall pay supplier/vendor for goods delivered and services rendered till the date of termination.

IN WITNESS WHEREOF THE PARTIES HERE TO have set and subscribed their respective hands and seals the day and year herein above mentioned.

a) SIGNED SEALED &DELIVEREDBY WITHIN NAMEDINSURANCECOMPANY

b) SIGNED SEALED &DELIVEREDBY WITHIN NAMED(BIDDER)

_____ _____

In the presence of

Witnesses:1

Witnesses:2

In the presence of

Witnesses:1___

Witnesses:2___

ANNEXURE -7

NDA FORMAT

(Should be on Rs.100/-stamp paper)

This confidentiality and non-disclosure agreement is made on the.....day of....., 20.....BETWEEN(Bidder), (herein after to be referred to as"-------")which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns a company incorporated under the Companies Act, 1956 and having its principal office at .....(address).

AND THE NEW INDIA ASSURANCE COMPANY LIMITED (hereinafter to be called "NIACL") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns having its Reg1stered Office at…….(address) on the following terms and conditions:

WHEREAS, in the course of the business relationship between the aforesaid parties, both the parties acknowledge that either party may have access to or have disclosed any information, which is of a confidential nature, through any mode and recognize that there is a need to disclose to one another such confidential information, of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure;

NOW THEREFORE, in consideration of the mutual promises contained herein, the adequacy and sufficiency of which consideration is hereby acknowledged and agreed, the parties hereby agree as follows: –

This Agreement shall apply to all confidential and proprietary information disclosed by one party to the other party, including information included in the caption 'Definitions' of this Agreement and other information which the disclosing party identifies in writing or otherwise as confidential before within thirty days after disclosure to the receiving party ("Confidential Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, electronically or through visual observation or by any other means to one party (the receiving party) by the other party (the disclosing party) provide information which has been disclosed in an intangible form shall reduce to writing within fifteen (15) business days for such information to be deemed as Confidential Information

1. DEFINITIONS

(a) CONFIDENTIAL INFORMATION means all the information of the Disclosing Party which is disclosed to the Receiving party pursuant to the business arrangement whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, inventions, techniques, processes, plans, algorithms, software programs, source code, semiconductor designs, schematic designs, business methods, customer l1sts, contacts, financial information, sales and marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs,

operations, strategies, inventions, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription l1sts, customer l1sts, photo files, advertising materials, contract quotations, charity contracts, documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, stat1stics, facts, figures, numbers, records, professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barr1sters, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors, Surveyors, Loss Assessors, Investigators, Forensic experts, Scient1sts, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Indian Evidence Act, 1872, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defenses taken before a Court of Law, Judicial For a, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Disclosing Party. The above definition of Confidential Information applies to both parties equally; however, in addition, without limitation, where the Disclosing Party is the NIACL, no information that is exempted from disclosure under section 8 or any other provision of Right to Information Act, 2005 shall at any time be disclosed by the Receiving Party to any third party.

(b) MATERIALS mean including without limitation, documents, drawings, models, apparatus, sketches, designs and l1sts furnished to the Receiving Party by the Disclosing Party and any tangible embodiments of the Disclosing Party's Confidential Information created by the Receiving Party.

2. COVENANT NOT TO DISCLOSE

The Receiving Party will use the Disclosing Party's Confidential Information solely to fulfill its obligations as part of and in furtherance of the actual or potential business relationship with the Disclosing Party. The Receiving Party shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Disclosing Party or its subsidiaries or affiliates, and shall not disclose the Confidential Information to any unauthorized third party. The Receiving Party shall not disclose any Confidential Information to any person except to its employees, authorized agents, consultants and contractors on a need to know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms at least as restrictive as those specified in this Agreement.

In this regard, the agreement entered into between the Receiving Party and any such person/s shall be forwarded to the Disclosing Party promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the Receiving Party shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information. The Receiving party shall use at least the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information, and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use. In no event, shall the Receiving Party take all reasonable measures that are lesser than the measures it uses for its own information of similar type. The Receiving Party and its Representatives will immediately notify the Disclosing Party of any use or disclosure of the Confidential Information that is not authorized by this Agreement. In particular, the Receiving Party will immediately give notice in writing to the Disclosing Party of any unauthorized use or disclosure of the Confidential Information and agrees to ass1st the Disclosing Party in remedying such unauthorized use or disclosure of the Confidential Information. The Receiving Party and its Representatives shall not disclose to any person

including, without limitation any corporation, sovereign, partnership, company, Association of Persons, entity or individual
(i) the fact that any investigations, discussions or negotiations are taking place concerning the actual or potential business relationship between the parties,

(ii) that it has requested or received Confidential Information, or
(iii) any of the terms, conditions or any other fact about the actual or potential business relationship.

This confidentiality obligation shall not apply only to the extent that the Receiving Party can demonstrate that:

a. The Confidential Information of the Disclosing Party is, or properly became, at the time of disclosure, part of the public domain, by publication or otherwise, except by breach of the provisions of this Agreement; or

b. was rightfully acquired by the Receiving Party or its Representatives prior to disclosure by the Disclosing Party;

c. was independently developed by Receiving Party or its Representatives without reference to the Confidential Information; or

d. the Confidential Information of the Disclosing Party is required to be disclosed by a Government agency, is the subject of a subpoena or other legal or demand for disclosure; provided, however, that the receiving party has given the disclosing party prompt written notice of such demand for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order prior to such disclosure.

e. is disclosed with the prior consent of or was duly authorized in writing by the disclosing party.

3. RETURN OF THE MATERIALS

Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the receiving party's counsel, solely for the purpose of proving the contents of the Information.

4. OWNERSHIP OF CONFIDENTIAL INFORMATION

The Disclosing Party shall be deemed the owner of all Confidential Information disclosed by it or its agents to the Receiving Party hereunder, including without limitation all patents, copyright, trademark, service mark, trade secret and other proprietary rights and interests therein, and Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as granting any rights to the Receiving Party, by license or otherwise in or to any Confidential Information. Confidential Information is provided "as is" with all faults. By disclosing Information or executing this Agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event, shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF

INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TOTHE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

5. REMEDIES FOR BREACH OF CONFIDENTIALITY

1. The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors) and that any unauthorized disclosure of any Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

2. The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

6. TERM

This Agreement shall be effective on the first date written above and shall continue in full force and effect for the term of the assignment and for a period of two years thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind both parties, and also their successors, nominees and assignees for the term of the assignment and for a period of two years thereafter.

7. GOVERNING LAW & JURISDICTION

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of law provisions. Any proceedings arising out of or in connection with this Agreement shall be brought only before the Courts of competent jurisdiction in Mumbai.

8. ENTIRE AGREEMENT

This Agreement sets forth the entire agreement and understanding between the parties as to the subject-matter of this Agreement and supersedes all prior or simultaneous representations, discussions, and negotiations whether oral or written or electronic. This Agreement may be amended or supplemented only by a writing that is signed by duly authorized representatives of both parties.

9. WAIVER

No term or provision hereof will be considered waived by either party and no breach excused by the Disclosing Party, unless such waiver or consent is in writing signed by or on behalf of duly Constituted Attorney of the Disclosing Party. No consent or waiver whether express or implied of a breach by the Disclosing Party will constitute consent to the waiver of or excuse of any other or different or subsequent breach by the Receiving Party.

10. SEVERABILITY

If any provision of this Agreement is found invalid or unenforceable, that part will be amended to achieve as nearly as possible the same economic or legal effect as the original provision and the remainder of this Agreement will remain in full force.

11. NOTICES

Any notice provided for or permitted under this Agreement will be treated as having been given when (a) delivered personally, or (b) sent by confirmed telecopy, or (c) sent by commercial overnight courier with written verification of receipt, or (d) mailed postage prepaid by certified or reg1stered mail, return receipt requested, or (e) by electronic mail, to the party to be notified, at the address set forth below or at such other place of which the other party has been notified in accordance with the provisions of this clause. Such notice will be treated as having been received upon actual receipt or five days after posting. Provided always that notices to the NIACL shall be served on the Information Technology Department of the Company's Head Office at Mumbai and a CC thereof be earmarked to the concerned Branch, Divisional or Regional Office as the case may be by RPAD &email.

IN WITNESS, WHEREOF THE PARTIES HERE TO have set and subscribed their respective hands and seals the day and year herein above mentioned.

a) SIGNED SEALED & DELIVEREDBYTHE WITHIN NAMED INSURANCE COMPANY

_____

In the presence of

Witnesses:1_____

Witnesses:2_____

b) SIGNED SEALED &DELIVEREDBY THE WITHIN NAMED(BIDDER)

_____

In the presence of

Witnesses:1_____

Witnesses:2_____

ANNEXURE –8

SPECIAL INSTRUCTIONS TO BIDDERS FOR E-TENDERING

1. Tender document with detailed terms and conditions is available on our Website **https://www.tenderwizard.com/NIAEPROC**. Interested parties may download the same and participate in the tender as per the instructions given therein, on or before the due date of the tender. The tender shall have to be submitted online through the e-Procurement system on **https://www.tenderwizard.com/NIAEPROC**

1. As a pre-requisite for participation in the tender, vendors are required to obtain a valid Digital Certificate of Class III (with both signing and encryption component) and above as per Indian IT Act from the licensed Certifying Authorities (For ex. N-codes, Sify, E-mudra etc.) operating under the Root Certifying Authority of India (RCIA), Controller of Certifying Authorities (CCA). The cost of obtaining the digital certificate shall be borne by the vendor. In case any vendor so desires, he may contact our e-Procurement service provider M/s. Antares Systems Ltd, Bangalore for obtaining the Digital Signature Certificate.

2. The Corrigendum / amendment , if any , shall be notified on the website https://www.tenderwizard.com/NIAEPROC In case any corrigendum/amendment is issued after the submission of the bid, then such vendors, who have submitted their bids, shall be intimated about the corrigendum/amendment by a system-generated email (In case of open tender corrigendum / amendment will be on the public dash board and no mail will be fired for the vendor who has not participated by that time). It shall be assumed that the information contained therein has been taken into account by the vendor. They have the choice of making changes in their bid before the due date and time.

3. Vendors are required to complete the entire process online on or before the due date of closing of the tender.

4. The Commercial/Price bid of only those vendors shall be opened whose Technical bid is found to be acceptable to us. The schedule for opening the price bid shall be advised separately.

5. Directions for submitting online offers, electronically, against e-Procurement tenders directly through internet:

    i. Vendors are advised to log on to the website (https://www.tenderwizard.com/NIAEPROC) and arrange to reg1ster themselves at the earliest.

    ii. The system time (1ST) that will be displayed on e-Procurement web page shall be the time considered for determining the expiry of due date and time of the tender and no other time shall be taken into cognizance.

iii. Vendors are advised in their own interest to ensure that their bids are submitted in e-Procurement system well before the closing date and time of bid. If the vendor intends to change/revise the bid already entered, he may do so any number of times till the due date and time of submission deadline.

However, no bid can be modified after the deadline for submission of bids.

iv. Once the entire process of submission of online bid is complete, the vendors are required to go to option own bid view through dashboard and take the print of the envelope receipt as a proof of submitted bid.

v. Bids / Offers shall not be permitted in e-Procurement system after the due date / time of tender. Hence, no bid can be submitted after the due date and time of submission has elapsed.

vi. No manual bids/offers along with electronic bids/offers shall be permitted.

2. Once the Commercial/Price bids are opened, vendors can see the rates quoted by all the participating bidders by logging on to the portal under their user ID and password and clicking on other bid view.

3. No responsibility will be taken by and/or the e-Procurement service provider for any delay due to connectivity and availability of website. They shall not have any liability to vendors for any interruption or delay in access to the site irrespective of the cause. It is advisable that vendors who are not well conversant with e-tendering procedures, start filling up the tenders much before the due date/times so that there is sufficient time available with him/her to acquaint with all the steps and seek help if they so require. Even for those who are conversant with this type of e-tendering, it is suggested to complete all the activities ahead of time. It should be noted that the individual bid becomes viewable only after the opening of the bid on/after the due date and time. Please be reassured that your bid will be viewable only to you and nobody else till the due date/ time of the tender opening. The non-availability of viewing before due date and time is true for e-tendering service provider as well as New India Assurance officials.

4. New India Assurance and/or the e-Procurement service provider shall not be responsible for any direct or indirect loss or damages and or consequential damages, arising out of the bidding process including but not limited to systems problems, inability to use the system, loss of electronic information etc.

5. In case of any clarification pertaining to e-Procurement process, the vendor may contact the following agencies/personnel:

1	FOR e-Tendering Support	M/s.Antares Systems Ltd.	080-40482100 lokesh.hr@etenderwizard.com raghuprashanth@etenderwizard.com sushant.sp@etenderwizard.com
2	For Tender Related Queries	The New India Assurance Co. Ltd	022-22708278 harish.gautam@newindia.co.in security.ho@newindia.co.in