File No. 10(21)/2022-NICSI

National Informatics Centre Services Incorporated

(A Government of India Enterprise under NIC)

Ministry of Electronics & Information Technology (MeitY)

Government of India

Request for proposal

for

Empanelment of Agencies

for

Providing Application Security Audit and Compliance Services

TENDER NO. NICSI/Application Security Audit/2023/05

1st FLOOR, NBCC TOWER,

15 BHIKAJI CAMA PLACE,

NEW DELHI – 110066.

TEL – 22900525, 34, 35 FAX – 26105212

TABLE OF CONTENT

1 FACTSHEET

Tender No.	NICSI/Application Security Audit/2023/05
Name of Organization	National Informatics Centre Services Inc. (NICSI)
Tender Type	Open Tender
Tender Category	Services
Type of Contract	Empanelment
Service Category	Application Security Audit and Compliance Services
Contract (Empanelment) Period	**Three (3) years** from the date of contract awarded and An additional **Two (2) year's** extension option.
Vendor Panel Size	**Up to 5(Five) Vendors**
Bid Security Deposit/Earnest Money Deposit (EMD)	**Bid Securing Declaration Form**
Bid Validity	**180 days** from the date of bid Opening
Date of Publication	**17.10.2023** at e-procurement portal site https://etenders.gov.in
Pre Bid queries submission last date:	**23.10.2023 till 17:00 Hours** ***Note**: Bidder who had sent their queries through e-mail (tender-nicsi@nic.in) will only be allowed to attend the pre-bid meeting.*
Pre-bid Meeting Date & Venue:	**25.10.2023 at 11:30 Hrs.** through Video Conference
Last date and time for Bid submission	**15.11.2023 at 15:00 Hrs.** Proposals that are received late WILL NOT be considered in this procurement process
Opening of Bids	**16.11.2023 at 15:30 Hrs.**
Opening of Financial Bids	Will be Informed Later after Technical Evaluation
Number of Packets	Two Packets Online bid submission as under: 1. **Packet-1 Technical Bid** (Bid Security Declaration/Eligibility & Technical Bid) 2. **Packet-2 Financial Bids** (Abridged & Detailed Financial)
Re-Bid Submission allowed?	**Yes (**Before last date of bid submission)
Bid Withdrawal allowed?	**Yes (**Before last date of bid submission)
Address for Communication	**Tender Division NICSI** National Informatics Centre Services Inc. 1stFloor, 15 NBCC Tower, Bhikaji Cama Place, New Delhi-110066 Email: tender-nicsi@nic.in , Phone: 011-22900525

2 *ABOUT NICSI*

The National Informatics Centre Services Inc. (NICSI) was set up in 1995 as a section 25 Company (now a Section 8 Company) under National Informatics Centre, Ministry of Electronics & Information Technology, Government of India to provide total IT solutions to the Government organizations. NICSI provides services for several e-Governance projects undertaken by NIC and MeitY.

Main Objectives:

- To provide economic, scientific, technological, social, and cultural development of India by promoting the utilization of Information Technology. Computer-Communication Networks, Informatics etc. by a spin-off of the services, technologies, infrastructure, and expertise developed by the NIC of the Government of India including its Computer-Communication Network, NICNET and associated infrastructure and services.

- To promote further development of services, technologies, infrastructure, and expertise supplementing that developed by NIC in directions which will increase the revenue earning capacity of NIC.

- To develop and promote value added computer and computer-communications services over the basic infrastructure and services developed by NIC including NICNET.

In furtherance of these objectives, NICSI has been providing various products & services to organizations in the Central Government, State Governments and PSUs etc. Products and Services include Hardware, Systems Software, Application Software, Software Development, Intra-Networking, Wide Area Networking, Video Conferencing, IT Consultancy, IT Implementation Support among others.

3 DEFINITIONS

In this document, the following terms shall have respective meanings as indicated:

- "**NICSI**" shall mean National Informatics Centre Services Incorporated, New Delhi. The term NICSI includes successors and assigns of NICSI.
- "**NIC**" shall mean National Informatics Centre, New Delhi.
- "**Client**" shall mean the department/organisation for which the order is being placed.
- **"e-Governance**" ICT (Information and Communication Technology) based projects in government sector
- "**RFP**" shall mean Request for Proposal, Tender Document or Bidding Document including the written clarifications issued by NICSI in respect of the RFP.
- "**Authorized Representative/Agency**" shall mean any person/agency authorized by NICSI.
- "**Contract**" shall mean the Work Order placed by NICSI on successful Bidder and all attached exhibits and documents referred to therein and all terms and conditions thereof together with any subsequent modifications thereto.
- **"Financial Year" (FY)** period from 1st of April till 31st of March of subsequent year.
- **"Specifications"** shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Bidding Documents.
- **"Bidder"** means the firm offering the solution(s), services and/or materials required in the RFP. The word Bidder when used in the pre award period shall be synonymous with Bidder, and when used after intimation of Successful Bidder shall mean the Successful Bidder, also called "Agency", on whom NICSI places Work Order for Delivery of services.
- **"Party"** shall mean NICSI or Bidder individually and "Parties" shall mean NICSI and Bidder collectively.
- "**Services"** means requirements defined in this document including all additional services associated thereto to be delivered by the Bidder.
- "**SME"** means subject matter expert is an individual with a deep understanding of a particular job, process, department, function, technology, machine, material, or type of equipment.
- **"SDLC"** means Software Development Life Cycle.
- **"CISO" means Chief Information Security Officer**
- **"DCISO" means Deputy Chief Information Security Officer**

4 SCOPE OF WORK

NICSI as part of the Application Security Audit and Compliance Services will empanel maximum of five agencies for the execution of work. The total number of websites/applications in the NIC network is around 13000 already hosted. However, this empanelment is primarily to cater audit of web sites, mobile applications, APIs, Data bases and Information security, Comprehensive security audit of applications for pre-launch and post launch by government departments/ministries/associated organisations either directly or through NICSI or by on-boarding through GEM.

In-Scope Location: The successful bidders must execute the activities at the following locations:

- Regional Centre of Excellence AppSec Centres at Lucknow, Guwahati, Bhubaneshwar, Jaipur, and Thiruvananthapuram

Assessment Process: All the selected agencies would be required to provide services for the allocated pool of Web Sites/Applications either separately in each category or as a combination as:

In-Scope Activities*:* Activities for Each Empaneled agency

Activities/Qualification
Broad Application Security Audit and Compliance Activities (including Web Application and its hosting infrastructure assessment, which includes but is not limited to OS, Web Server, Development framework, Database, Application testing, SSL certificate provisioning, Hardening as well as other required security compliance checks.)
Application Penetration Testing (including hosting infrastructure assessment)
Optional Activity: Comprehensive Security Assessment relevant to a project / setup

NIC hosts around 13,000 portals / websites / applications / APIs for the Government. These are hosted currently at the National Data Centers at Delhi, Hyderabad, Pune, Bhubaneshwar and the NIC State centers. Most applications cater to the requirement of respective Government Departments/Ministries. These are either developed/managed in-house by NIC or are developed and managed by the Departments themselves. The possibility of attack is due to flaws in the design, development, and deployment of application software. The vulnerabilities thus created may be exploited by intruders with malicious intent to cause defacements, data corruption, data/information leakage and disruption in service continuity etc. To track such vulnerabilities, Security Audits and penetration testing are required to be performed followed by subsequent hardening aimed to mitigate the vulnerabilities and strengthening the security of the applications and their environment. As a policy, all websites / applications hosted at the NIC Data centers must go through a complete security audit process before they can be onboarded or whenever an alteration/addition is made to the application. The security audit / penetration testing is undertaken at various stages before, during and after hosting.

Before hosting

- Security audit of Web Application as per latest OWASP standard & NIC guidelines and submission of report for required remediation
- Second level testing for verification of closing all the discovered vulnerabilities
- Issuance of Certificate of 'safe for hosting'

During Hosting

- Configuration review / SSL deployment
- Random Penetration Testing of hosted application

After Hosting

- Black Box Testing at regular intervals
- Penetration Testing at regular intervals
- Periodic Hosting Infrastructure assessment

The Terms and Conditions laid down by NIC/NICSI based on specific requirements need to be strictly adhered upon by the empaneled agencies.

These and related activities are being undertaken by in house professionals of the Cyber Security Audit Group (Application Security Audit Division) and Centre of Excellence AppSec Centres of NIC. Considering the magnitude of the work, this specialized group needs the services of organizations who can manage end to end security for these Web Applications/APIs.

This tender aims for empanelment of agencies for providing Application Security Audit and Compliance Services at NIC HQs or at other centres of NIC or in other government domains. The methodology for application audit to be followed shall be based mainly on the Open Web Application Security Project (OWASP) model. However, there may be necessary variations in approach as required by NIC and each auditor is expected to comply with all NIC laid down policies and procedures for conducting application security audits.

4.1 BROAD APPLICATION SECURITY AUDIT AND COMPLIANCE ACTIVITIES

The security auditors shall be performing some or all the following activities:

1. Exposure to Secured design concept adoption early in the development cycle (SDLC)
2. Identify the application-level vulnerabilities on applications hosted at test site / production site based on the latest top 10 OWASP or other known vulnerabilities
3. Daily or on demand application scans
4. An audit of the hosting environment along with the application to ascertain any vulnerabilities in the environment where the application is hosted
5. The auditor must have his own tools to conduct audit activities
6. The activity should additionally include but not limited to the following which are vulnerable to the web applications:
    - Password strength on authentication pages
    - Scan Java Script for security vulnerabilities

- File inclusion attacks
- Web server information security
- Malicious File Uploads
- Hosting Infrastructure vulnerabilities

7. Provide recommendations for remediation of identified vulnerabilities
8. Submit detailed reports for each iteration of audit and a final report showing all vulnerabilities as closed. The report should contain found vulnerabilities, vulnerability description and solution. It needs to be ensured that audit of each allocated assignment is completed.
9. Follow a specific format for reports, if so, required by NIC
10. The Certification for each applications / websites/mobile apps/web service/Thick Client(executable)/IoT based services tested may be provided as "Safe for Hosting"
11. Accept responsibility for declaring the websites / URLs / mobile applications/Thick Client(executable)/IoT based services free from known vulnerabilities
12. Any Application(s) directory/web service being used in the application but not directly linked to the web site
13. Any other activity concerning security audit related aspects; not essentially covered by work-areas outlined above
14. Key Areas Web Application Security Audit and Compliance would cover:
    - Access to sensitive data - Sensitive files such as website backup files or configuration files containing passwords may be present on the web server and accessible to unauthorized individuals
    - Administrative Access - Default or easily guessable passwords may be used to gain access to the administrative section of the website
    - Authentication - Obtain unauthorized access to data or functionality due to authentication weakness
    - Backdoors - Identify malicious entry paths that provide administrative access into the application or system
    - Cookie poisoning - Change cookie data to access sensitive information or impersonate another user
    - Forceful browsing - Access a web page or directory directly that should only be reached as an authenticated user
    - Hidden field manipulation - Modify hidden field values to manipulate web application functionality or access sensitive data
    - Informational - View unauthorized data, such as personally identifiable information of another user
15. Recommended frequency of Web Application Security Audit and Compliance
    - Every Web application must undergo assessment once in a year (or as per the cyber security policy of NIC), or upon change or as per recommendation from CLIENT
    - Application when going live must undergo Security Testing Assessment; the findings in the assessment will be closed and reviewed by assessment team for closure verification.

16. Key Areas of mobile application testing (as per OWASP Mobile Top 10) should cover:
    - Static and Dynamic Analysis testing
    - Insecure Data Storage – Sensitive data such as backdoors, API key or configuration files containing passwords may be present on the Mobile app and accessible via reverse engineering.
    - Privacy concerns – Assess the application's compliance with regards to privacy according to the Mobile Marketing Association's (MMA) Privacy Policy Framework.
    - Insufficient Transport Layer Protection –Complete lack of encryption for transmitted data. Weakly encrypted data in transit.
    - Client-Side Injection – Some familiar faces (XSS, HTML Injection, SQL injection). Injection attacks such as SQL Injection on client devices can be severe if your application deals with more than one user account on a single application or a shared device or paid-for-only content.
    - Poor Authorization and Authentication –To ensure only authorized users can perform allowed actions within their privilege level. As some applications rely solely on immutable, potentially compromised values (IMEI, IMSI, UUID).
    - Cookie poisoning – Change cookie data to access sensitive information or impersonate another user.
    - Improper Session Handling –Mobile applications sessions are generally much longer. They use generally HTTP Cookies, OAuth Tokens, SSO Authentication Services.
    - Weak Server-Side Controls –Applies to the backend services.
    - Insecure Data Storage –Sensitive data left unprotected, applies to locally stored data + cloud synced.
    - Web Service should also be in the scope of audit, which interacts with mobile APK.
    - Reverse engineering and code tampering check.
17. API testing (as per OWASP API Top 10)
18. Recommended frequency of Mobile Application Security
    - Every Mobile application/API testing must undergo assessment once in a year (or as per the cyber security policy of NIC), or upon change or as per recommendation from CLIENT
    - Application when going live must undergo through assessment process. Findings in the assessment must be closed and reviewed by assessment team for closure verification.

    Coverage: All web applications hosted over NICNET and other government domains and related Mobile Apps/APIs

19. Acquisition of expertise in taking up security compliance testing in emerging areas like (i) microservices and (ii) Data security controls

4.2 APPLICATION PENETRATION TESTING

i. Vulnerability assessment and pen-testing for deployed and running applications/mobile apps.
ii. The activity must include both the manual and automated assessment.
iii. This activity should be done every quarter or on a 6-month basis
iv. The infrastructure will include the database, application server and the OS.
v. The activity must include identification and evaluation of vulnerability present at the infrastructure level for application. The same must be represented by detailed report of the vulnerability with an adequate recommendation.
vi. Need to ensure validation of Digital Assets (Domain) validation of Web Applications/ Mobile Apps /APIs taken up for testing.
vii. Vulnerability Assessment of application hosting infrastructure and run time application platform.
viii. Application Security Vulnerability assessment (automated scanning and manual testing in non-intrusive mode)
ix. The website/web application access for audit through VPN and will be carried out on production environment without any impact on performance
x. The Mobile Apps (with brief usage description) and main APIs used may also be disclosed, so that the same can be taken up for assessment.
xi. The audit activity needs to be completed in fixed timeline period as per the specified timeline.
xii. The security issues traced during internal audit (for Application and hosting infrastructure related issues) needs to be taken up for fixation by respective Ministry/Department (within 1 month period from the date of report submission).
xiii. Revalidation of fixing of audit findings before final submission of audit report, on assurance of fixation or after completion of fixation period.
xiv. In case of some audit related queries with respect to any Application, the respective HOD/DCISO shall facilitate requisite information to Security Auditors/NIC AppSec team.
xv. A detailed test report must be prepared as part of penetration testing
xvi. Before submission of final detailed test report, on assurance of fixation or after completion of fixation period, only one round of revalidation check would be taken by the auditor concerned.
xvii. Coverage: All web applications/APIs hosted over NICNET and other government domains and related Mobile Apps

4.3 COMPREHENSIVE SECURITY ASSESSMENT

The comprehensive infrastructure assessment is to preview the required "scope of work" outlined for respective NIC/NICSI projects which apart from audit of complete Deployment architecture plan and workflow of hosted applications, also includes compliance security testing of all in-line network devices, network security devices, operating systems, Web Servers, Hosting frameworks, Business Logic compliance and Data Security control checks, Mobile Apps, Malware analysis, Forensic analysis, UIDAI

compliance requirements, APIs and databases related with that NIC/NICSI project requirement.

Security Audit through CSA activity should be taken up as per the outlined scope and emphasise on the broader and granular coverage of critical ICT NIC/NICSI projects. The audit process shall adhere to a well-defined checklist document as per the defined scope of CSA requirement.

5 *ELIGIBILITY CRITERIA*

i. For eligibility criteria, bidders may refer Annexure-4: Eligibility Compliance Sheet, Annexure-5: Technical Evaluation Criteria.

ii. The bids consisting of documents in support of the eligibility criteria and those required as per "Annexure-4: Eligibility Compliance Sheet and Annexure-5: Technical Evaluation Criteria" should be uploaded electronically and document properly page numbered and indexed. Undertaking for subsequent submission of any of the required document/Deviations will not be entertained under any circumstances. NICSI reserves the right to seek clarifications on the bids submitted by the bidders.

6 BIDDING PROCESS

Bidders are advised to study the Tender Document carefully. Submission of the Bid shall be deemed to have been done after careful study and examination of Tender document (including corrigendum, if any) all instructions, eligibility norms, terms, and requirement specifications with full understanding of its implications. Bids not complying with all the given clauses in this tender document or failure to furnish all information required or submission of a bid not substantially responsive in every respect will be at bidder's risk and may result in the rejection.

6.1 AVAILABILITY OF TENDER

i. The tender document is available at NICSI e-procurement site http://etenders.gov.in
ii. Prospective bidders desirous of participating in this tender may view and download the tender document free of cost from the above-mentioned website.
iii. The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in rejection of the proposal.
iv. Online bidding can be done through NICSI e-Procurement System at NICSI e-procurement site http://etenders.gov.in

6.2 PRE-BID MEETING

i. NICSI shall hold a pre bid meeting with the prospective bidders as per the schedule provided in **Section- FACTSHEET**. Queries received from the bidders regarding bidding conditions, bidding process, item specifications, evaluation criteria, etc., in writing, or over email (preferably in an excel file), **up till two days prior to the pre bid meeting**, shall be addressed. The queries can be sent to NICSI through email at **tender-nicsi@nic.in**
ii. **Only those pre-bid queries which are received in the following prescribed format shall be entertained:**

Company name		**M/s……..**		
S. No.	**Relevant Section / Annexure of RFP**	**RFP Page No.**	**Relevant Content from RFP**	**Vendor's Query / Comment**

iii. NICSI is not bound to clarify any query received after the day as described above. NICSI will review every query and on due consideration will issue corrigendum (if require). However, NICSI does not undertake to answer each individual query (ies). Bidders shall not assume that their unanswered queries have been accepted by NICSI.

iv. Due to Pandemic (Covid-19) scenario, the Pre-Bid meeting shall be organized through Video Conference. All interested prospective bidders (one authorized representative) may participate in the pre-bid meeting.

v. To join the Pre-bid through video conference, interested bidders are required to provide following details on email id at "tender-nicsi@nic.in**" two days before the schedule pre-bid meeting date**. The joining link/credentials will be shared over the email provided by the bidder.

Name of the company: M/s _____

Name of the authorised representatives to attend VC: _____

Email Id of the representative: _____

Contact No. of representative: _____

It is the responsibility of the prospective bidders to have appropriate environment/connectivity for smooth participation.

6.3 AMENDMENT OF TENDER DOCUMENTS

i. At any time prior to the last date for receipt of bids, NICSI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the tender documents through an amendment/corrigendum. The amendment will be notified through CPP portal, which will be binding on all prospective bidders to consider the amendment and accordingly submit their proposal/ quotation.

ii. To give prospective bidders reasonable time to take the amendment into account in preparing their bids, NICSI may, at its discretion, extend last date for the receipt of bids.

iii. No bid may be modified after the last date for receipt of bids. No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the bidder in the bid. Withdrawal of a bid during this interval may result execution of Bid Securing Declaration.

6.4 LANGUAGE OF BID

The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and NICSI, shall be written in English. Supporting documents and printed literature furnished by the bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in English. For the purposes of interpretation of the bid, the translation shall govern. Information supplied in another language without proper translation shall be rejected.

6.5 BIDDING COST

The Bidder shall bear all costs associated with the preparation/submission of the Bid. NICSI will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6.6 BID SECURITY DEPOSIT/EARNEST MONEY DEPOSIT DECLARATION

a. The Bidders shall submit "**Bid Security Deposit Declaration Form**" as per the format mentioned in **Annexure-3: FORMAT FOR BID SECURITY DECLARATION FORM/EARNEST MONEY DEPOSIT** through uploaded onto the CPP Portal as per bid submission section.

b. The bids without Bid Security Deposit Declaration Form in the prescribed format as mentioned above, will be summarily rejected.

c. In case the Bid Securing Declaration is not received by the stipulated time then the Purchaser reserves the right to forth with and summarily reject the Proposal of the concerned Bidder without providing any opportunity for any further correspondence by the concerned Bidder.

7 BID SUBMISSION

i. Bidder shall adhere to the timelines as mentioned in the Section: FACT SHEET. No bids shall be accepted post the deadline as mentioned in this schedule.

ii. Bids submitted in Online will be only considered for the tender opening process and further evaluation.

iii. Incomplete bids will be rejected straight away and will not be considered.

7.1 ONLINE BID SUBMISSION

i. Online bids (complete in all respect) must be uploaded on https://etenders.gov.in latest by the time & date mentioned in **the Section FACTSHEET.**

ii. The Online bids should be submitted as under with mentioned two packets online:

Packet Number	Documents to be uploaded	Packet File Format
Packet-1 **(Technical Bid)**	The files should be saved in a PDF version as *'packet1<BidderName>".pdf* **1.** Scanned copy of Covering Letter in Company Letter Head as per **Annexure-2:** COVERING LETTER FOR BID duly sealed & signed (PDF) **2.** Scanned copy of Bid Securing Declaration Form duly sealed and signed as per the format mentioned in **Annexure-3:** FORMAT FOR BID SECURITY DECLARATION FORM/EARNEST MONEY DEPOSIT. (PDF) **3.** Scanned copy of Original Power of Attorney letter in a Non-Judicial Stamp Paper of at-least Rs.100/- or Board Resolution in Letter Head in original in case of Registered Limited Companies or **Original Authorization in Letter Head** in case of Partnership Firm Or **Original Self Certificate** in Letter Head in case of Proprietorship naming/indicating the person authorized to sign the bid (PDF). **4.** Scanned copy of **Bidder's Profile** as per **Annexure-1: Bidder's profile** duly filled in, signed, and stamped along with all supporting documents. **5.** Scan copy of duly filled signed and stamped **Eligibility Compliance Sheets** as per **Annexure-4** and all the **supporting/mandated documents** and **Annexures** required for eligibility criteria.	**PDF**

	6. Scan copy of duly filled signed and stamped **Technical Evaluation Criteria** as per **Annexure-5** and all the **supporting/mandated documents** and **Annexures** required for technical evaluation criteria. *Note: The PDF file not containing the above documents or containing the financial bid in the explicit/implicit form will lead to rejection of the bid.*	
Packet-2 **(Financial Bid)**	Financial Bids to be uploaded as: **1.** As per BoQ: **GTV** Financial Bid as per **Annexure-6: ABRIDGED FINANCIAL BID** (in .xls format) **And** **2. Detailed financial bid** as per **Annexure-7: DETAILED FINANCIAL BID** (in .pdf format). The Detailed Financial Bid scanned pdf files, then should be saved in a RAR '*Detailed_Fin <Bidder's Name>".RAR* *All the bids documents duly signed by the authorized signatory of the company and stamped with company seal*	**XLS** **&** **RAR**

Note: The bidders will be invited for presentation as per the technical evaluation criteria mentioned in Annexure 5: Technical Evaluation Criteria. The decision of TEC will be final in this regard.

Instructions for Online Submission

I. Instructions for Packet-1

a. All the bid documents must be duly signed by the authorized signatory of the company and stamped with company seal.

b. It shall be the sole responsibility of the bidder to check (and double-check) the page number referencing made for supporting documents in the checklist indicated under Annexure-4: Eligibility Compliance sheet and Annexure-5: Technical Evaluation Criteria Sheet. No relevant information/document should be left, whether listed above or not

c. Bidder must provide all documents mandated for bidder's profile, prequalification criteria and for technical evaluation criteria.

d. All pages of the bid being submitted must be sequentially numbered by the bidder

e. Relevant referencing shall be done by the bidder, clearly indicating all page numbers where supporting documents are provided.

f. The document should have a Table of Contents indicating page no. where supporting document are placed. All pages in the bid document should be sequentially numbered, stamped, and signed by the authorized signatory.

II. Instructions for Packet-2

a. The Bidder must upload the BoQ as per the format provided on CPP portal. The bidder must adhere to terms and conditions and fill in the required details as required in BoQ.

b. The bidder must strictly follow the prescribed format as mentioned in the detailed Financial Bids.

c. The bidder shall quote only the GTV value in Abridged Financial Bid as derived from in Detailed Financial Bid for which bid is being quoted.

d. During financial opening, only the Abridged Financial Bid shall be opened for determining the L1 bidder based on the GTV value.

e. Any other itemized financial details mentioned in the Abridged Financial Bid may lead to rejection of the bid.

f. All the bid documents should be duly signed by the authorized signatory of the company and stamped with company seal.

7.2 GENERAL INSTRUCTIONS FOR BID SUBMISSION

i. NICSI will not be responsible for any delay on the part of the vendor in submission of bid.

ii. Bids submitted by Fax/E-mail etc. shall not be considered. No correspondence will be entertained on this matter.

iii. Conditional Bids shall not be accepted on any ground and shall be rejected straightway. (A bid is conditional when bidder submits its bid with his own conditions & stipulations extraneous to the terms and conditions specified in this tender) If any clarification is required, same should be obtained before submission of bids i.e., during pre-bid meeting.

iv. No bids will be accepted after the expiry of the deadline as stated in the Fact Sheet.

v. In case, the day of bid submission is declared Holiday by Govt. of India, the next working day will be treated as day for submission of bids. There will be no change in the timings.

vi. All pages of the bid being submitted must be signed by the authorized signatory, stamped, and sequentially numbered by the bidder irrespective of the nature of content of the documents. Un-signed & un-stamped bid may be summarily rejected.

vii. At any time prior to the last date for receipt of bids, NICSI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the Tender Document by publishing an amendment/corrigendum. The amendment will be notified on NICSI's CPP portal https://etenders.gov.in and should be taken into consideration by the prospective agencies while preparing their bids. It is the responsibility of the bidder to check website for any such notice/changes and submit its bid accordingly.

viii. To give prospective agencies reasonable time to take the amendment into account in preparing their bids, NICSI may, at its discretion, extend the last date for the receipt of bids. No bid may be modified after the last date for receipt of bids. No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified in the tender. Withdrawal of a bid during this interval may result in execution of Bid Securing Declaration.

ix. Printed terms and conditions of the vendors will not be considered as forming part of their bid. In case any terms and conditions of the tender document is/are not acceptable to the bidder or submitted any deviation, the bid shall be rejected summarily.

x. Bids not submitted as per the specified format and nomenclature may be rejected.

xi. Ambiguous/Incomplete/Illegible bids may be out rightly rejected. Not quoted bids shall be consider as non-responsive and shall be rejected.

xii. Any alteration/overwriting/cutting in the bid should be duly countersigned else it will be out rightly rejected.

xiii. Submission of the Bid will be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and required specifications in the tender document with full understanding of its implications. Bids not complying with all the given clauses in this tender document are liable to be rejected. Failure to furnish all information required in the tender Document or submission of a bid not substantially responsive to the tender document in all respects will be at the vendor's risk and may result in the rejection of the bid.

xiv. Tender process will be over after the issuance of empanelment letter(s) to the selected agency (ies).

xv. For additional instructions, refer to the Section Bid Evaluation, Technical Evaluation and Financial Bid Evaluation, etc.

xvi. Submission of false/forged documents will lead to execution of Bid Securing Declaration and blacklisting of agency for a minimum period of 3 years from participating in NICSI tenders.

7.3 BID OPENING

a. NICSI shall convene a bid opening session as given in the **FACTSHEET**, where one representative from the agencies, who have successfully uploaded the bid, can participate.

b. NICSI will download the **Packet-I** from e-tender portal at first. Agencies' representatives can remain present during the bids download process.

c. Bids will then be passed on to duly constituted Technical Evaluation Committee (TEC).

d. Financial bids of only those bidders whose bids are found qualified by the Evaluation

Committee as per both Pre-Qualification & Technical criteria will be opened in the presence of the bidder's representatives subsequently for further evaluation.

e. Financial bids, original and revised, if any, of only technically qualified agencies shall be opened on a notified date and time in the presence (physical/ Video Conference) of agency's representatives who chose to remain present.

f. Financial bids will then be passed on to a duly constituted Financial Evaluation Committee (FEC) for evaluation.

7.4 BID VALIDITY

a. All the bids must be valid for a period of **180 days** from the date of bid opening.

b. If necessary, NICSI shall seek extension in the bid validity (as required) validity period.

c. The bidders, not agreeing for such extensions will be allowed to withdraw their bids.

8 BID EVALUATION

i. Any effort by a bidder to influence NICSI's bid evaluation, bid comparison or contract award decisions may result in the rejection of the bidder's bid and execution of Bid Securing Declaration. No enquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the Committee / its authorized representative and office of NICSI can make any enquiry / seek clarification from the bidders, which the bidders must furnish within the stipulated time else the bids of such defaulting bidders will be rejected.

ii. NICSI reserves the right to accept any bid, and to cancel/abort the Tender process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder or bidders, of any obligation to inform the affected bidder of the grounds for NICSI's action and without assigning any reasons.

iii. Printed terms and conditions of the vendors will not be considered as forming part of their bid. In case any terms and conditions of the tender document are not acceptable to the bidder, the bid shall be summarily rejected.

8.1 TECHNICAL EVALUATION

a. A duly constituted Technical Evaluation Committee (TEC) will first evaluate bidders based on Annexure-4: Eligibility Compliance Sheet of this tender.

b. The TEC will examine the eligibility documents of the bidders as per the tender specifications. Bids of the bidders, not satisfying the eligibility criteria shall be rejected.

c. Only bidders who satisfy all the conditions of the eligibility criteria completely will be considered for further technical evaluation.

d. The TEC will further evaluate the documents of the eligible bidders as per the Annexure-5: Technical Evaluation Criteria.

e. The presentation made by the bidders will be technically evaluated and marked as part of marking scheme provided in Annexure-5: Technical Evaluation Criteria and the decision of TEC will be final in this regard.

f. If required by the TEC, the bidders shall also assist the TEC in getting relevant information from the bidders' references. Agencies failing to adhere to the specified time limit will not be considered for further evaluation.

g. The TEC may decide to visit the premises of the bidder to verify the information submitted by them. For this the bidder shall extend all cooperation, shall present the documents desired by the TEC at the premises and adhere to the time targets set by the TEC. NICSI will bear all expenditure of the TEC visits.

h. To qualify in the Technical Evaluation, a bidder must obtain a minimum score of 70% of the total marks in the Annexure-5: Technical Evaluation Criteria.

i. Financial bids of only the technically qualified bidders will be opened.

j. All technically qualified bidders i.e., with minimum score of 70% in technical evaluation are then ranked as T1, T2.... so on based on score.

8.2 FINANCIAL EVALUATION

a. On a designated day and time, the **Abridged Financial Bids (Annexure-6: Abridged Financial Bid)** of only those Bidders who satisfy all conditions of the eligibility criteria and have passed the Technical Evaluation Stage will be opened electronically in the presence of the representatives of the technically qualified bidding companies.

b. The lowest quoting vendor (L1) in each category will be the bidder with the lowest Gross Total Value (GTV) among all the quoted eligible GTV in the **Abridged Financial Bids (Annexure-6: Abridged Financial Bid).**

c. The detailed financial bid **Annexure-7: Detailed Financial Bid** of only the lowest quoting bidder for each category shall be opened and will be evaluated by a duly constituted Finance Evaluation Committee (FEC).

d. The bidder with the Second Lowest GTV among the Abridged Financial Bids will be the L2 bidder and will then be asked to match the item-wise price of L1, category wise to be placed on the panel (within a timeframe prescribed by NICSI). If L2 does not agree, L3, L4 & so on…will be asked to match the item-wise price of L-1. Thus, by way of successive opportunity a **panel of vendors as per defined category wise** will be formed.

e. If none of L2, L3, L4…. agree to match the L1 rates then L1 shall be the sole vendor on the panel. The decision of NICSI arrived at, as per above will be final for empanelment and no representation of any kind shall be entertained.

f. If NICSI considers necessary, revised Financial Bids could be called from the eligible Bidders, before opening the original financial bids for recommending final empanelment.

g. In the event of revised financial bids being called the revised bids should not be higher than the original bids, otherwise the bid shall be rejected. There will be no negotiation regarding the financial/ commercial bid.

h. Quoting '0' (Zero) value of an item with a view to subverting the tender process shall be rejected straight away and execution of Bid Securing Declaration of such bidders.

i. If there is a mismatch between values quoted in figures and words, the value quoted in words shall prevail.

j. A Financial Evaluation Committee (FEC) would scrutinize the commercial bids. Bids found lacking in strict compliance to the commercial bid format shall be rejected straightaway.

k. If there is only one bid, NICSI reserves the right to process the single bid or take

recourse to the process of re-tendering.

l. Arithmetical error will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price with quantity/weightage, the unit price shall prevail, and the total price shall be corrected. If the bidder does not accept the correction of the errors, its bid will be rejected, and Bid Securing Declaration will be executed. If there is a discrepancy between words and figures, the amount in words will prevail.

m. If any discrepancy found in L1 bid during financial evaluation process, then L2 bidder will be considered as L1. Similarly, if any discrepancy is also found with L2 bidder, L3 bidder will be considered as L1. This procedure will continue until the L1 bidder is selected. Similarly, the process will continue till empanelment of specified no. of bidders.

n. NICSI reserves the right to use this tender to service its clients'/NIC/NICSI needs.

o. The rates quoted should be as per industry standards for the prescribed experience. The bids in which the bidder quote NIL charges/considerations, such bid will be treated as unresponsive and will not be considered.

p. Bids of those bidders whose Financial Bid's Gross Total Value (GTV) have a deviation **beyond 30% (thirty Percent)** on either side from the Average GTV of all the technically qualified bidders would be disqualified.

q. NICSI reserve the right to reject bid of a bidder in view of wide disparity in the item wise rates.

9 *EMPANELMENT*

9.1 SIGNING OF CONTRACT

a. Empanelment will be initially for a period of three years, extendable for next two more years on year-to-year basis solely at the discretion of NICSI on same terms and conditions or additional mutually agreeable conditions.

b. NICSI will have a panel of vendor up to 5 (Five) empaneled vendors

c. The empanelment can be used by both NICSI and NIC.

d. The rates finalized shall remain valid during empanelment/extended empanelment.

e. The incidental expenses of execution of agreement/contract shall be borne by the empanelment vendor.

f. After empanelment, selection procedure for issuance of Work Order / Purchase Order will be at the sole discretion of NICSI/User Department. The Bidder will provide services as per NICSI/User Department's requirements.

g. Escalation Matrix for Problem solving: The Empaneled agency should provide an escalation matrix for problem resolution to the user by providing the Names, Designations, Contact Number(s) and Email ID's of the persons to be contacted. The Empaneled agency should also provide website URL for such purpose.

h. On written communication from NICSI for having qualified for empanelment the bidder shall sign contract (letter of empanelment) within 7 days of such communication. Failing which the offer shall be treated as withdrawn and execution of Bid Securing Declaration.

i. Empaneled agencies must honor all tender conditions and adherence to all aspect of fair-trade practices in executing the purchase orders placed by NICSI on behalf of its clients. Failing this, NICSI may execute of Bid Securing Declaration and stop further participation of such agency (ies) for three years in NICSI tendering process.

j. In the event, an Empaneled Company or the concerned division of the Company is taken over /bought over by another company, all the obligations and execution responsibilities under the agreement with NICSI, should be passed on for compliance by the new company in the negotiation for their transfer.

k. During the empanelment, NICSI may ask the agency to submit the supporting documents which may be required to ensure that the tender terms and conditions are fulfilled.

l. The agency should not assign or sublet the empanelment or any part of it to any other agency in any form. Any such attempt shall result in termination of empanelment and

forfeiture of security deposit, revocation of bank guarantees (including the ones submitted for other work orders)

m. NICSI may, at any time, terminate the empanelment by giving written notice to the Empaneled agency without any compensation, if the Empaneled agency becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to NICSI.

n. Reasons for rejecting tender/bid will be disclosed to a bidder only where enquiries are made.

o. NICSI may verify the CA certificate along with required supporting documents submitted as part of bid by the bidder 'as and when required' during bid evaluation or/and the course of empanelment.

9.2 SECURITY DEPOSIT FOR EMPANELMENT

a. Selected bidder(s) will submit the security deposit in the form of an Account Payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, Bank Guarantee, Bankers Cheque from a Commercial bank, or online payment in an acceptable form for the duration of empanelment plus 3 months or extended period if any (with 3 months add on period), in favour of NICSI, New Delhi.

b. **The Security Deposit for this category is mentioned as under:**

Security Deposit Amount	Security Deposit Amount (words)
INR 25 Lakhs	**Rupees Twenty-Five Lakh**

c. NICSI will have the right to forfeit the security deposit if the empaneled agency fails to meet the terms and conditions of the tender document or perform any other obligation under the contract, fails to execute the work orders issued by NICSI.

d. Apart from this NICSI also reserves the right to cancel the empanelment of the selected agency in case of repeated default.

e. Empaneled agencies shall be required to submit Security Deposit within 14 days of issuance of Empanelment letters by NICSI.

f. Security Deposit should remain valid for a period of 60 (Sixty) days beyond the date of completion of all contractual obligations of supplier i.e., (Empanelment/Extension duration).

g. In the event wherein the Empanelment is extended by NICSI beyond 2 years, the selected agency shall ensure submission of a fresh Security Deposit within 14 days of issuance of letter for extension of Empanelment by NICSI.

h. The Validity of this Security Deposit shall also be for an additional period of 60 (Sixty) days beyond the period of extension of Empanelment.

i. The BG will be released without any accrued interest after the empanelment or execution of all pending POs whichever is later.

9.3 PERFORMANCE BANK GUARANTEE (PBG)

a. The selected Service Provider shall be required to furnish a **Performance Bank Guarantee (PBG)** equivalent to **3% (Three Percent)** of the Work Order/Purchase Order value.

b. PBG will be in the form of an Account Payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, an unconditional and irrevocable Bank Guarantee, Bankers Cheque from a Commercial bank or online payment in an acceptable form drawn in the name of National Informatics Centre Services Inc. (NICSI), New Delhi.

c. PBG should remain a period of 60(Sixty days) beyond the date of completion of all contractual obligations of the supplier

d. PBG must be submitted after award of contract but before signing of contract.

e. The successful service provider must renew the PBG on same terms and conditions for the period up to contract including extension period, if any.

f. PBG would be returned (without any accrued interest) only after successful completion of tasks/deliverables assigned to them as per PO and only after adjusting/recovering any dues recoverable/payable from/by the Service Provider on any account under the contract.

g. NICSI will have the right to forfeit the PBG along with the Security Deposit without assigning any reasons if selected agency defaults or deemed to have defaulted or in case of non-acceptance of purchase orders and thereafter the empanelment will be cancelled.

h. Empaneled agencies shall be required to give PBG as per the following timelines (For work related to Manpower mode and Project Mode). For projects duration between 0-6 months, PBG should be submitted within 15 days of issuance of PO by NICSI and for projects duration greater than 6 months, PBG should be submitted within 30 days of issuance of PO by NICSI.

i. In the event of default/delay in submission of PBG within the stipulated time, the agency shall be liable for a penalty amounting to 0.1% (Zero Point One Percent) of the PO value per day delay with a Maximum penalty capping of 10% of PO value.

j. In the event wherein a PO is released by NICSI for project renewal, or a fresh PO is released, the bidder shall ensure extension/submission of PBG with 15 days of issuance of the PO.

9.4 INFORMATION SECURITY

a. Service Provider shall not carry and/or transmit any material, information, application details, equipment or any other goods/material in physical or electronic form, which are proprietary to or owned by NICSI, out of premises without prior written

permission from NICSI.

b. Service Provider acknowledges that NIC's business data and other NICSI proprietary information or materials, whether developed by NICSI or being used by NICSI pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to NICSI; and Service Provider agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Service Provider to protect its own proprietary information.

c. Service Provider recognizes that the goodwill of NICSI depends, among other things, upon Service Provider keeping such proprietary information confidential and that unauthorized disclosure of the same by Service Provider could damage NICSI and that by reason of Service Provider's duties hereunder. Service Provider may come into possession of such proprietary information, even though Service Provider does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. Service Provider shall use such information only for the purpose of performing the said services.

d. Service Provider shall, upon termination of this agreement for any reason, or upon demand by NICSI, whichever is earliest, return all information provided to Service Provider by NICSI, including any copies or reproductions, both hardcopy and electronic.

e. The Appointed agency will not disclose any information, to anyone in any form about software, hardware, network topology, IP Schema, and network security policies of NICSI. Information disclosure to anyone shall be only with prior written consent of NIC/NICSI/User. In case of User Department/NIC/NICSI or project requirement(s), a separate "Non-Disclosure Agreement" Annexure-9: Proforma for Non-Disclosure Agreement shall be signed within 1 week after receiving work order.

9.5 CONFIDENTIALITY

Empanelled bidder and their personnel shall not, either during the term or after expiration of this contract, disclose any proprietary or confidential information relating to services, contract or business or operations of NICSI or its clients without prior written consent of NICSI.

10 PLACEMENTS OF WORK ORDERS

i. NIC/NICSI may place the work orders on empaneled agencies for its own requirement or for its projects on behalf of its clients as per empanelment for the items which have direct prices. Other items such as CSA etc., Work order will be released equivalent Man-Days values.

ii. NICSI may also on-board this empanelment on GEM platform along with derived prices for placement of Work orders through GEM (as per instructions of MeitY) as and when provisions made in GEM platform.

iii. This tender is for empanelment of multiple agencies. In view of NICSI's order on Procurement Preference Policy, preference shall be given to L1 bidder of such category for distribution of projects (purchase orders)/work in that category. However, NICSI/User shall have right to choose any other eligible bidder for allotment of projects (purchase orders)/work considering various parameters like performance, location, mix of project etc. or any other factors depend on situations.

iv. In case, NICSI has to select the agency for awarding the work order, preference may be given to L1 bidder.

v. Work Order may encompass the complete scope of work or may require few services. Depending on requirement, the work orders may be placed to anyone of the empaneled agency; more than one depending on the project requirement or the TOR may be given to more than one empaneled agency for their proposals for the specific scope of work using the L1 rates. In the document, work order can be read as work order/Purchase order.

vi. On receipt of request from a User department, NICSI would inform the User Department/ Agency/Institution about the Empaneled agencies and GFR compliant procedure followed in the empanelment.

vii. In case User Department clearly and specifically states in writing the name of a particular agency, NICSI may assign the work to that agency. In such cases, the responsibility for adhering to relevant financial/procurement rules would be that of Department concerned.

viii. Users/Departments/Ministries may also place work orders through GEM after onboarding this empanelment over GEM. In such case, Terms and Conditions of GEM contract may prevail along with T&C of this tender/empanelment.

ix. Terms of Reference/Scope of Work will be shared among all Empaneled agencies and would be invited by the Committee to make presentations and submission of technical proposal and financial effort estimate in a separate sealed envelope regarding project under consideration. Presentations may be evaluated objectively, based on which most suitable agency may be assigned the work by NICSI, on the recommendation of above Committee. There should be full participation and involvement of the User Department in the process of selection of agency. For assignment of work to

Empaneled agencies, above mentioned Standard Operating Procedure (SOP) is followed or implementation of new guidelines from time to time.

x. Proposal of selected agency along with supporting document/minutes of meeting are then forwarded to NICSI by user department for issuance of Proforma Invoice (PI).

xi. Once the requisite funds are transferred to NICSI against issued PI, Work Order will be placed on selected agency as per terms and conditions of empanelment and scope of work.

11 PAYMENT TERMS

i. Payment will be made in Indian Rupees only.

ii. All empaneled agencies should furnish details of the location from where they are going to raise their Bills / Invoices to NICSI, New Delhi.

iii. All the empaneled agencies shall have to raise their Bills / Invoices in the Pre-receipted bills which shall be submitted in triplicate in the name of:

National Informatics Centre Services Inc.,

Hall No. 2&3, 6th Floor, NBCC Tower,

15 Bhikaji Cama Place, New Delhi –110066

iv. Payment to the agency will be released quarterly based on the pro rata amount of work done. The empaneled agencies will submit pre-receipted bills in triplicate for quarterly period along with certificate from the NIC Coordinator or User regarding satisfactory performance and an SLA compliance sheet related to the services.

v. Payment will be made after deducting penalty amount, if any. The maximum penalty will not exceed 10% of the work order due to the agency.

vi. GST would be paid extra as may be applicable from time to time.

vii. PBG will have to be renewed for such further periods till satisfactory services has been provided by the empaneled agency and there after the PBG will be returned to the empaneled agency. If bills, complete in all aspects are submitted with all relevant documents as defined above, NIC/NICSI will ensure that the payment are made to empaneled agency within 30 (thirty) days from the date of bill submission.

viii. Payments shall be subject to deductions of any amount for which the empanelled agency is liable under the empanelment. Further, all payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the Income-Tax Act, 1961 and any other taxes.

ix. In case the submission of bills to NIC/NICSI, along with the necessary documents i.e., WO's/BG's etc., is delayed by the empanelled agency beyond 30 (Thirty) days from the date of issue of bill or delivery of materials etc., whichever is earlier, the entire liability towards payment of interest/penalty to the tax authorities would be on the cost of respective empaneled agency so that NIC/NICSI is not burdened unnecessarily with this amount. The entire amount will be deducted from the payment due, to the respective empaneled agency.

x. All payments will be made through RTGS only.

12 SLA AND PENALTY

<table>
<tr><th>S. No.</th><th>Item</th><th>Penalty</th></tr>
<tr><td colspan="3">Application Security compliance Assessment and Reporting</td></tr>
<tr><td></td><td>Adequate accuracy rate for website/ portal/ Mobile App/ application security compliance assessment and reporting of vulnerabilities</td><td>The Auditing agency must submit the Audit/ PT/ Comprehensive Security assessment report and maintain adequate accuracy rate, failing which the penalty as per the following slabs will be applicable.
<table>
<tr><th>Percentage of Vulnerabilities Reported</th><th>Applicable Penalty</th></tr>
<tr><td>>=95%</td><td>None</td></tr>
<tr><td>>=90% but <95%</td><td>2% of the respective work orde</td></tr>
<tr><td>>=85% but <90%</td><td>3% of the respective work orde</td></tr>
<tr><td>>=80% but <85%</td><td>4% of the respective work orde</td></tr>
<tr><td><80% but >=60%</td><td>8% of the respective work orde</td></tr>
<tr><td><60%</td><td>20% of the respective work orc</td></tr>
</table></td></tr>
<tr><td colspan="3">Level of Assessment</td></tr>
<tr><td>1</td><td>Web Application compromised due to Vulnerabilities existing at the time of Audit/PT/ Comprehensive Security assessment but not discovered by the Auditors</td><td>If any website/portal/Mobile App/ application security compliance tested by an auditor of an empaneled Auditing agency deployed at NIC/NICSI is defaced or corrupted and is proved to be caused through a vulnerability not highlighted in the audit report, the concerned Auditing agency shall be charged penalty of 5% of respective work order (of the respective slabs) for per reported vulnerability as per the following:
Repository of audited sites will be maintained. Vulnerability reported will be related to known vulnerabilities as on date of report submission, defacement due to new vulnerabilities will not be considered here.</td></tr>
<tr><td>2</td><td>Vulnerabilities reported during follow up Audit/PT/ Comprehensive Security assessment or third-party audit</td><td>At any stage, during the follow up audit done by the second empaneled auditor, if it is found that the bidder did not report one or more observations (which existed during the time when initial Audit/PT/ Comprehensive Security assessment was performed by the bidder), however the follow up audit will be conducted solely at the behest of the user/NIC, and the modalities involved will be discussed with the user in advance
OR
At any stage, NIC/NICSI may also involve another empaneled agency to re-validate the observations reported by the bidder.
<table>
<tr><th>S. No.</th><th>Type of Vulnerability Identified</th><th>Penalty</th></tr>
<tr><td>1.</td><td>High (exploitable)</td><td>5% of the respective work or per reported vulnerability</td></tr>
</table></td></tr>
</table>

		2.	Medium	2% of the respective work orde per reported vulnerability
Delay in Mobilization of Resources and Deliverables				
3	Time taken in starting the Audit/PT/Comprehensive Security assessment process	The Auditing agency must provide the required auditing resource(s)/start the execution of Audit/PT/Comprehensive Security assessment process within 2 weeks of receiving the work order from NIC/NICSI, failing which penalty at the rate of **1% of the respective work order for every week of delay**. In case of any delay due to natural calamities or any other dependencies relaxation can be decided only by NIC/NICSI/User department.		
4	Time taken in providing the replacement	The Auditing agency must provide the required auditing resource(s) for execution of Audit/PT/Comprehensive Security assessment process within 1 week of absence of resource placed at NIC/NICSI, failing which penalty at the rate of **1% of the respective work order for every week of delay**.		
5	Delay in Audit/PT/ Comprehensive Security assessment process	Any delay in completion of the Audit/PT/Comprehensive Security assessment process not attributable to the user will result in a penalty of 0.2% of the work order per day. The time taken for the Audit/PT/ Comprehensive Security assessment will differ according to website and the time and effort will have to be finalized by the user in consultation with the audit agency		
6	Submission of Audit/PT/ Comprehensive Security assessment reports	The audit reports must be submitted within a week of the completion of Audit/PT/Comprehensive Security assessment failing which a penalty of 0.2% of the work order per day will be charged to the agency		
7	Sub-Contracting by the bidder	Sub-Contracting of resources is not permitted and if found guilty then a penalty of INR 5,00,000 (Rupees Five Lakh only) would be applicable on the agency at each instance and appropriate legal action would be initiated against it.		
8	Breach of confidentiality	In case of breach of confidentiality agreement and contractual terms of this RFP, the Bidder will be subjected to proceedings as per law of the land. The penalties in this regard will be as per the instructions of court or out of court settlement between NICSI and the Bidder. And the PBG submitted by agency shall be uncashed.		
9	Data Theft	For every data theft incident involving the auditing resource deployed by the Bidder a penalty of INR 5,00,000 (Rupees Five Lakh only) shall be imposed along with punishment applicable under the legal provision of the country and the state prevailing at the point of time.		

Note – *Any delay not attributable to the audit agency will not result in penalty for the agency*

13 GENERAL TERMS AND OTHER CONDITIONS

13.1 GENERAL CONDITIONS

a. The empanelment under this tender is not assignable by the selected vendor. The selected vendor shall not assign its contractual authority to any other third party.

b. As a matter of policy and practice and on the basis of Notification published in Gazette of India dated 14th March, 1998, it is clarified that services and supplies of the vendor selected through this tender can be availed by both National Informatics Centre [NIC] and National Informatics Centre Services Incorporated [NICSI], as the case may be depending on the project, and the selected vendor shall be obliged to render services / supplies to both or any of these organizations as per the indent placed by the respective organization. In other words, the selection procedure adopted in this tender remains applicable for NIC as well, and in the event of rendering services / supplies to NIC, the selected vendor shall discharge all its obligations under this tender vis-à-vis NIC.

c. Any default or breach in discharging obligations under this tender by the selected vendor while rendering services / supplies to NICSI, shall invite all or any actions / sanctions including execution of Bid Securing Declaration, security deposit stipulated in this tender document. The decision of NICSI/NIC arrived at as above will be final and no representation of any kind will be entertained on the above. Any attempt by any vendor/empanelled bidder to bring pressure of any kind, may disqualify the vendor/empanelled bidder for the present tender and the vendor/empanelled bidder may also be liable to be debarred from bidding for NICSI/NIC tenders in future for a period of at least three years.

d. All terms and conditions governing prices and supply given in this tender, as applicable to NICSI, will be made equally applicable to NIC.

e. NICSI reserves the right to modify and amend any of the stipulated condition/criterion given in this tender, depending upon project priorities vis-à-vis urgent commitments. NICSI also reserves the right to accept/reject a bid, to cancel/abort tender process and/or reject all bids at any time prior to award of empanelment, without thereby incurring any liability to the affected agencies on the grounds of such action taken by the NICSI.

f. Any default by the bidders in respect of tender terms & conditions will lead to rejection of the bid with execution of Bid Securing Declaration /forfeiture of Security Deposit.

g. The decision of NICSI arrived during the various stages of the evaluation of the bids is final & binding on all vendors. Any representation towards these shall not be entertained by NICSI. Reasons for rejecting a bid will be disclosed only when an enquiry is made by the concerned bidder.

h. In case the empanelled vendor vendor/empanelled bidder is found in-breach of any condition(s) of tender or supply order, at any stage during the course of project deployment period, the legal action as per rules/laws will be taken.

i. Any attempt by vendor vendor/empanelled bidder to bring pressure towards NICSI's decision making process, such vendors shall be disqualified for participation in the present tender and those vendors may be liable to be debarred from bidding for NICSI tenders in future for a period of three years.

j. Printed/written conditions mentioned in the tender bids submitted by vendors will not be binding on NICSI.

k. Upon verification, evaluation/assessment, if in case any information furnished by the vendor is found to be false/incorrect, their total bid/Contract shall be summarily rejected and no correspondence on the same, shall be entertained.

l. NICSI will not be responsible for any misinterpretation or wrong assumption by the vendor, while responding to this tender.

13.2 MICRO, SMALL & MEDIUM ENTERPRISES DEVELOPMENT ACT, 2006

a. If a bidder falls under the Micro, Small & Medium Enterprises Development Act, 2006, then a copy of the valid certificate must be provided to NICSI. Further, the bidder must keep NICSI informed of any change in the status of the company.

b. Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organization or the concerned Ministry or Department are liable to get following benefits:

i) Issue of tender sets free of cost (zero Tender Fee)

ii) Exemption from payment of earnest money (zero EMD)

c. The bidder is required to submit a copy of the registration certificate to NICSI. Further, the bidder must keep NICSI informed of any change in the status of the company.

d. NICSI shall continue concluding this empanelment with agencies as per existing procedures. The responsibility shall lie with the government user departments and agencies under their control to comply with the criteria prescribed in the notified policies & guidelines.

13.3 PREFERENCE TO MAKE IN INDIA

a. In conformance to the DOT MII and MIII Guidelines to promote Make in India, the bidders are encouraged to include products made in India in their bid.

b. All the Bidders to note that Govt. of India had taken out Preference for Make in India (PMI) policy in 2015 and subsequently respective nodal ministries have taken out GOs detailing out the PMI and local content (LC).

c. Bidders are encouraged to go through the GOs issued by DoT and MeitY. Few of these are as follows, but not limited to:

- No. P-45014/33/2021-BE II, dated 20th December 2022
- No. P-45021/102/2019-BE-II Part (I), dated 4th March 2021
- No. P-45021/2/2017-PP (BE-II) dated 4th June 2020
- No. P-45021/2/2017-PP (BE-II) dated 29th May 2019
- No. P-45021/2/2017-PP (BE-II) dated 15th June 2017

- No. 18-10/2017-IP dated 29th August 2018

13.4 LIMITATION OF LIABILITY

a. Except conditions enumerate in Indemnity Clause, the damage caused by the empanelled agency to User Department / NICSI / NIC under any work order issued pursuant to this empanelment, the empanelled agency shall be liable to end user / NICSI / NIC for damage and loss to the maximum extent of the work order value. However, the total value of damages, during the period of empanelment that can be levied on the empanelled agency shall not exceed the total contract value of the work entrusted to them.

b. Empanelled Agency shall be liable for all acts of omission and commission by its employees deployed under this empanelment and User Department / NIC / NICSI stand and insulation against aggrieved third-party complaints against any civil or criminal actions of the empanelled agency or its employees.

c. Limitation of liability: In no event will empanelled agency be liable for any incidental, indirect, special or consequential costs or damages including, without limitation, downtime cost, unavailability of or damage to data; or software restoration. To the extent allowed by local law, these limitations shall apply regardless of the basis of liability, including negligence, misrepresentation, breach of any kind, or any other claims in contract, tort or otherwise."

13.5 INDEMNITY

a. The selected agency shall indemnify and defend the NICSI/User departments against all third-party claims of infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied software/ hardware, documents, other artefacts, deployed resources and related services or any part thereof ("Deliverables"). The selected agency shall have no obligations with respect to any claims to the extent such claim results from:

(i) the selected agency's compliance with NICSI/User departments specific technical designs, specifications or instructions where the selected agency has notified NICSI / User department in writing (with proper reasons) prior to implementation of such specific technical designs, specifications or instructions that the implementation of such specific technical designs, specifications or instructions will result in infringement claims.

(ii) inclusion in a Deliverable of any content or other materials provided by NICSI/User departments and the infringement relates to or arises solely from such NICSI/User departments materials or provided material.

(iii) (modification of a Deliverable after delivery by the selected agency to NICSI/User departments if such modification was not made by or on behalf of the selected agency and the claim arises solely due to such modification.

(iv) operation or use of some or all of the Deliverable in combination with materials not provided by the selected agency and the claim arises solely due to such reason; or

(v) use of the Deliverable for any purposes for which the NICSI/ User department have been advised in advance in writing that the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided by the selected agency; or

(vi) use of a superseded release of some or all of the Deliverables or NICSI/User departments‟ failure to use any modification of the Deliverable furnished under the contract including, but not limited to, corrections, fixes, or enhancements made available by the selected agency provided that such modifications or new releases are made available by selected agency free of cost and the use of such modifications or new releases does not adversely impact the performance / service levels

b. NICSI/User department stand indemnified from any employment claims that the hired manpower /Resources / agency's manpower may opt to have towards the discharge of their duties in the fulfilment of the purchase orders.

c. Each party also stands indemnified from any compensation arising out of accidental loss of life or injury sustained by such party's manpower while discharging their duty towards fulfilment of the purchase orders caused by the negligence or willful misconduct of the other Party or its agents and representatives.

13.6 LABOUR LAWS

a. The vendor shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the manpower employed thereof.

b. Wherever necessary, the vendor shall apply for and obtain license as provided under Section 12 of Contract Labour (Regulation and Abolition) Act, 1970, and strictly comply with all the terms and conditions that the licensing authority may impose at the time of grant of license. NICSI shall not be held responsible for any breach of the license terms and conditions by the vendor.

c. The vendor shall be solely responsible for the payment of wages to the deployed manpower and ensure its timely payment thereof.

d. The vendor shall duly maintain a register giving particulars of the deployed manpower, nature of work, rate of wages, etc.

e. The vendor shall also ensure compliance to the following labour legislations:

(i) Minimum Wages Act *

(ii) Employees Provident Fund Act *

(iii) Employees State Insurance Act *

(iv) Workmen's Compensation Act, if the ESI Act does not apply *

*Applicable as per respective state

f. The vendor shall be solely responsible to adhere to all the rules and regulations relating to labour practices and service conditions of its workmen and at no time shall it be the responsibility of NICSI.

g. The vendor shall indemnify NICSI against any liability incurred by NICSI on account of any default by the vendor or manpower deployed by it.

h. Neither the vendor nor his workmen can be treated as employees of NICSI for any purposes. They are not entitled for any claim, right, preference, etc. over any job/regular employment of NICSI. The vendor or its workmen shall not at any point of time have any claim whatsoever against NICSI.

i. If the User Department / NICSI / NIC so recommends, a deployed resource must be replaced by the vendor within a period of 5 working days.

j. Medical benefits should be provided by the agency to the manpower deployed

13.7 TERMINATION FOR INSOLVENCY

NICSI may at any time terminate the purchase order/empanelment by giving four weeks written notice to the vendor vendor/empaneled bidder, without any compensation to the vendor vendor/empaneled bidder, if the vendor vendor/empaneled bidder becomes bankrupt or otherwise insolvent.

13.8 FORCE MAJEURE

If at any time, during the continuance of the empanelment, the performance in whole or in part by either party of any obligation under the empanelment is prevented or delayed by reasons of any war, hostility, acts of public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics quarantine restrictions, strikes, lockouts or acts of God (hereinafter referred to as "events"), provided notice of happenings of any such event is duly endorsed by the appropriate authorities/chamber of commerce in the country of the party giving notice, is given by party seeking concession to the other as soon as practicable, but within 21 days from the date of occurrence and termination thereof and satisfies the party adequately of the measures taken by it, neither party shall, by reason of such event, be entitled to terminate the empanelment/contract, nor shall either party have any claim for damages against the other in respect of such nonperformance or delay in performance, and deliveries under the empanelment/contract shall be resumed as soon as practicable after such event has come to an end or ceased to exist and the decision of the purchaser as to whether the deliveries have so resumed or not, shall be final and conclusive, provided further, that if the performance in whole or in part or any obligation under the empanelment is prevented or delayed by reason of any such event for a period exceeding 60 days, the purchaser may at his option, terminate the empanelment.

13.9 TERMINATION OF CONTRACT

NICSI reserves the right to suspend any of the services and/or terminate this agreement in one or more of the following circumstances by giving 30 days‟ notice in writing:

(i) TERMINATION FOR INSOLVENCY, DISSOLUTION ETC.

NICSI may at any time terminate the contract by giving written notice to the selected agency without compensation to the selected agency, if the selected agency becomes bankrupt or otherwise insolvent or in case of dissolution of firm or winding up of company, provided that such termination will not prejudice or effect any right of action or remedy which has accrued thereafter to NICSI.

(ii) TERMINATION FOR DEFAULT:

NICSI may without prejudice to any other remedy for breach of contract, (including forfeiture of security deposit, Performance Bank Guarantee) by written notice of default sent to the Empaneled agency, terminate the contract in whole or in part after sending a notice to the Empaneled agency in this regard.

a) If the Empanelled agency fails to accept the Purchase Order(s).

b) If the Empanelled agency fails to deliver services within the time-period specified in the purchase orders or during any extension thereof granted by NICSI.

c) If the Empanelled agency fails to meet any other terms and conditions under the contract.

(iii) TERMINATION FOR CONVENIENCE

NICSI may by written notice, sent to the selected agency, terminate the work order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination will specify that termination is for NICSI"s convenience, the extent to which performance of work under the work-order and/or the contract is terminated and the date upon which such termination becomes effective. NICSI reserves the right to cancel the remaining part and pay to the selected agency an agreed amount for partially completed Services.

(iv) TERMINATION PROCESS

1) Upon occurrence of an event of default as set out in above clauses, NICSI will deliver a default notice in writing to the other party which shall specify the event of default and give the Empanelled agency an opportunity to correct the default.
2) At the expiry of notice period, unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the agreement.

(v) Payments for all satisfactorily completed services till the time of termination shall be made to the vendor in the event of termination.

13.10 ARBITRATION

NICSI and the empaneled agency will make every effort to resolve amicably, by direct negotiation, any disagreement or dispute arising between them under or in connection with the agreement/wok-order. If any dispute will arise between parties on aspects not covered by this agreement, or the construction or operation thereof,

or the rights, duties or liabilities under these except as to any matters the decision of which is specially provided for the general or the special conditions, such dispute will be referred to panel of three arbitrators, one to be appointed by each party and the third to be appointed by the Ministry of Electronics & Information Technology (MeitY) and the award of the arbitration, as the case may be, will be final and binding on both the parties. Such arbitration will be governed in all respects by the provision of the Indian Arbitration and Conciliation Act, 1996 or amended later and the rules there under and any statutory modification or re-enactment, thereof. The arbitration proceedings will be held in New Delhi, India.

1. If a dispute arises out of or in connection with this contract, or in respect of any defined legal relationship associated therewith or derived there from, the parties agree to submit that dispute to arbitration under the ICADR Arbitration Rules, 1996.
2. The Authority to appoint the arbitrator(s) shall be the International Centre for Alternative Dispute Resolution (ICADR).
3. The International Centre for Alternative Dispute Resolution will provide administrative services in accordance with the ICADR Arbitration Rules, 1996.

13.11 CONCILIATION

If a dispute arises out of or in connection with this contract, or in respect of any defined legal relationship associated therewith or derived there from, the parties agree to seek an amicable settlement of that dispute by Conciliation under the ICADR Conciliation Rules, 1996.

The Authority to appoint the Conciliator(s) shall be the International Centre for Alternative Dispute Resolution (ICADR).

The International Centre for Alternative Dispute Resolution will provide administrative services in accordance with the ICADR Conciliation Rules, 1996.

13.12 APPLICABLE LAW

a. The vendor vendor/empanelled bidder shall be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing.
b. All disputes in this connection shall be settled in Delhi jurisdiction only.
c. NICSI reserves the right to cancel this tender or modify the requirement at any stage of Tender process cycle without assigning any reasons. NICSI will not be under obligation to give clarifications for doing the aforementioned.
d. NICSI reserves the right that the work can be allocated to any of the empanelled vendors.
e. NICSI also reserves the right to modify/relax any of the terms & conditions of the tender by declaring / publishing such amendments in a manner that all prospective vendors / parties to be kept informed about it.

f. NICSI, without assigning any further reason can reject any tender(s), in which any prescribed condition(s) is/are found incomplete in any respect and at any processing state.

g. NICSI also reserves the right to award work orders on quality / technical basis, which depends on quality, capability and infrastructure of the firm.

h. All procedure for the purchase of stores laid down in GFR and DFPR shall be adhered-to strictly by the NICSI and subordinates and Bidders are bound to respect the same.

13.13 NON-SOLICITATION

The Empaneled agency and User Department / NICSI each agree that during the term, Empaneled agency personnel or User Department / NICSI employee is associated with the services under the Contract and for a period of twelve months after such person ceases to be so associated, neither the Empaneled agency nor User Department / NICSI shall, directly or indirectly, solicit for hire or knowingly hire or retain such personnel of the other party as an employee or independent contractor, except with prior written consent of the other party.

13.14 CONFIDENTIALITY

a. Selected agency (the "Receiving Party") shall acknowledge and agree to maintain the confidentiality of Confidential Information (as hereafter defined) provided by the NICSI/ user department (the "Disclosing Party"). The Receiving Party shall not disclose or disseminate the Disclosing Party's Confidential Information to any person other than those employees, agents, contractors, subcontractors and licensees of the Receiving Party, or its affiliates, who have a need to know it in order to assist the Receiving Party in performing its obligations, or to permit the Receiving Party to exercise its rights under the Contract Agreement.

b. The term "Confidential Information", as used herein, shall mean all business strategies, plans and procedures, proprietary information, software, tools, processes, methodologies, data and trade secrets, and other confidential information and materials of the Disclosing Party, its affiliates, their respective clients or suppliers, or other persons or entities with whom they do business, that may be obtained by the Receiving Party from any source or that may be developed for the Disclosing Party as a result of the Contract Agreement.

c. The provisions respecting confidentiality shall not apply to the extent, but only to the extent, that the information or document is: (i) already known to the Receiving Party free of any restriction at the time it is obtained from the Disclosing Party, (ii) subsequently learned from an independent third party free of any restriction and without breach of this provision; (iii) is or becomes publicly available through no wrongful act of the Receiving Party or any third party; (iv) is independently developed by the Receiving Party without reference to or use of any Confidential Information of the Disclosing Party; or (v) is required to be disclosed pursuant to an applicable law, rule, regulation, government requirement or court order, or the rules of any stock exchange (provided, however, that the Receiving Party shall

advise the Disclosing Party of such required disclosure promptly upon learning thereof in order to afford the Disclosing Party a reasonable opportunity to contest, limit and/or assist the Receiving Party in crafting such disclosure).

d. The obligations under this clause shall survive for three years from termination or expiration of this Contract.

e. The work order/contract with the user department may define more stringent confidentiality obligations depending on the nature of information / data being shared. In such event, the more stringent obligations shall prevail.

13.15 INTELLECTUAL PROPERTY RIGHTS

i) Subject to the other provisions contained in this Clause, the Empanelled Agency shall agree that all deliverables created or developed by the Empanelled Agency, specifically for the User Department/NICSI/NIC, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre (hereafter NIC).

ii) The User Department/NICSI/NIC shall acknowledge that:

a. In performing services under the Contract, the Empanelled Agency may use Empanelled Agency's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by the Empanelled Agency prior to or independent of the services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the services hereunder, ("the Empanelled Agency's Pre-Existing IP").

b. Notwithstanding anything to the contrary contained in the Contract, the Empanelled Agency shall continue to retain all the ownership, the rights title and interests on all the Empanelled Agency's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Empanelled Agency from using the Empanelled Agency's Pre-Existing IP in any manner.

c. If any of the Empanelled Agency's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the Empanelled Agency hereby grants to the User Department/NICSI/NIC a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple Categories, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.

d.

i. NIC being the owner of all the IPs created in the deliverables, except the Pre- Existing IPs of the Empanelled Agency used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer,

share, deploy, develop, modify or any such act that the user department/NICSI/NIC may require or find necessary for its purpose. The IP rights of the /NIC shall indefinitely subsist or continue in all future derivatives of the deliverables.

ii. The Empanelled Agency shall have no claims whatsoever on the deliverables and all the IPs created in deliverables or in course of development of the applications except its Pre-Existing IPs for which it shall grant all authorizations to the User department/NICSI/NIC for use as detailed in the Clause(c) above.

iii. Except as specifically and to the extent permitted by the Empanelled Agency, the User department/NICSI/NIC will not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source code of the Agency's Pre-Existing IP, or separate Empanelled Agency's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.

e. The User Department/NICSI/NIC shall warrant that the materials provided by the User Department/NICSI/NIC to Empanelled Agency for use during development or deployment of the application shall be duly owned or licensed by the User Department/NICSI/NIC.

13.16 INTEGRITY PACT

a. In compliance with the Central Vigilance Commissioner Circular No. 06/05/21 dated 3rd June 2021 regarding adaptation of Integrity Pact- Revised Standard Operating Procedure to ensure transparency, equity and competitiveness in public procurement, the Bidder(s)/Vendor(s)/Prospective vender(s) are required to sign an Integrity Pact (IP) with NICSI.

b. The pact essentially an agreement between the Bidder(s)/ Vendor(s)/Prospective vender(s) and the NICSI, committing the persons/Officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract. Only those bidders, who commit themselves to such a pact with the NICSI, would be considered competent to participate in the bidding process.

c. The bidders are required to sign the Integrity pact with the NICSI. The format for integrity pact will be shared with bidder later.

d. Further, any violation of Integrity pact would entail disqualification of the Bidder(s)/Vendor(s) and exclusion from NICSI's future bidding process for one year and execution of Bid Securing Declaration Form of such Bidder(s)/Vendor(s).

14 SPECIAL TERMS AND CONDITIONS

1. The agency must not use this empanelment anywhere on its own, without taking prior permission from NICSI. Any work order placed with reference to this empanelment must be executed through NICSI only.
2. Start-up category vendors that have been previously empanelled with NICSI to provide the same services are not permitted to take part in this tender process.

15 ANNEXURES

The Annexures are given in the following pages.

ANNEXURE-1: BIDDER'S PROFILE

<On Company's Letter Head>

Name of the Bidder (in CAPITAL letters only): _____

Date of Incorporation in India as: _____

Registration No: _____

Complete Address with PIN: _____

Contact Person Name:				
Designation:				
Telephone:				
Fax:				
E-mail:				
Goods & Service Tax No. (GSTN)				
Whether Bidder is MSME: *(Yes/No)* *(if Yes, please attach Udyam Registration certificate)*	If yes, a) Type of Enterprise: _____ b) Udyam Registration No.: _____			
PAN No.:				
ISO Certification(s):				
CMMI Certification:				
Total Number of employees				
Annual Turnover (in INR Crores)	**2020-21**	**2021-22**	**2022-23**	**Average Turnover**
Overall Annual turnover				
From Security Audit				
Whether Bidder is blacklisted: *(Yes/No)*				
Whether any Litigation Arbitration/ proceeding: *(Yes/No)*				

Note: *Copies of the supporting documents should be attached along with the proposal.*

Signature (Bidder Seal)

In the capacity of

Duly authorized to sign proposals for and on behalf of:

ANNEXURE-2: COVERING LETTER

<To be submitted on the letterhead of the bidder>

<Place>
<Date>

To
The Managing Director,
National Informatics Centre Services Incorporated (NICSI)
1st Floor, NBCC Tower,
Bhikaji Cama Place, New Delhi-110066

Subject: Submission of Bid for Empanelment of Tender No. …….

Dear Sir,

This is to notify that our company is submitting technical bid in response to Tender No <…….*Tender No*……> for <……*Name of the Tender*……...> for <……*Name of the Category*……...> Primary & Secondary contact for our company are as follows:

<M/s Company Name>	Primary Contact	Secondary Contact
Name		
Title		
Address		
Phone		
Mobile		
Fax		
E-mail		

We are responsible for communicating to the NICSI in case of any change in the Primary or/and Secondary contact information mentioned above. We shall not hold NICSI responsible for any non-receipt of bid process communication in case such change of information is not communicated and confirmed with NICSI on time.

We are submitting our bid for _____ as per the scope and requirements of the tender document:

By submitting the proposal, we acknowledge that we have carefully read all the sections of this tender document including all forms, scheduled and appendices hereto, and are fully informed to all existing conditions and limitations. We also acknowledge that the company agrees with terms and conditions of the tender and the procedure for bidding and evaluation.

Deviations:

We declare that all the services shall be performed strictly in compliance with the Tender Document. Further, we agree additional conditions, if any, found in the bid documents, other than those stated in the tender document, shall not be given effect to.

Bid Pricing:

We do hereby confirm that our bid prices exclusive all taxes, as applicable on the last date of submission of bid. We further declare that the prices stated in our proposal are in accordance with your terms & conditions in the bidding document.

Qualifying Data:

We confirm having submitted in qualifying data as required by you in your tender document. In case you require any further information/documentary proof in this regard before evaluation of bid, we agree to furnish the same in time to your satisfaction.

We confirm that information contained in this response or any part thereof, including documents and instruments delivered or to be delivered to NICSI are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part misled NICSI in its evaluation process.

We fully understand and agree that on verification, if any of the information provided here is found to be misleading the evaluation process or result in unduly favors to our company in evaluation process, we are liable to be dismissed from the selection process or termination of the contract during the empanelment with NICSI.

We understand that you are not bound to accept the lowest or any bid you may receive.

Have/undertake to open within 60 days of our empanelment, branch offices in the locations as stipulated in

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Yours sincerely,

On behalf of [bidder's name]
Authorized Signature [In full and initials]:
Name & Title of signatory:
Name of Firm:
Address:
Seal/Stamp of bidder:

Place:

Date:

ANNEXURE-3: FORMAT FOR BID SECURING DECLARATION FORM/ EARNEST MONEY DEPOSIT (EMD)

<*On Company's Letter Head*>

Date: _____ Tender No.: __xxxxxxxxxxxxx_____

To (*insert complete name and address of the purchaser*)

I/We. The undersigned, declare that:

I/We understand that, according to your conditions, bids must be supported by a Bid Securing Declaration.

I/We accept that I/We may be disqualified from bidding for any contract with you for a period of one year from the date of notification if I am /We are in a breach of any obligation under the bid conditions, because I/We

a. have withdrawn/modified/amended, impairs or derogates from the tender, my/our Bid during the period of bid validity specified in the form of Bid; or
b. have been notified of the acceptance of our Bid by the purchaser during the period of bid validity
    i. fail or reuse to execute the contract, if required, or
    ii. fail or refuse to furnish the Performance Security, in accordance with the instructions to Bidders.

I/We understand this Bid Securing Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the earlier of

i. the receipt of your notification of the name of the successful Bidder; or
ii. thirty days after the expiration of the validity of my/our Bid.

Signed: (*insert signature of person whose name and capacity are shown***)**

in the capacity of (*insert legal capacity of person signing the Bid Securing Declaration***)**

Name: (*insert complete name of person signing he Bid Securing Declaration*)

Duly authorized to sign the bid for an on behalf of: (*insert complete name of Bidder***)**

Dated on _____ day of _____ (insert date of signing)

Corporate Seal (where appropriate)

(Note:** In case of a Joint Venture, the Bid Securing Declaration must be in the name of all partners to the Joint Venture that submits the bid**)

ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)

This states the eligibility criteria essential for qualifying as a prospective bidder for this tender.

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no. where document occurs in the bid
1.	The bidder should be a company registered in India under the relevant act such as Companies Act 1956/ 2013, **or** a partnership registered under the India Partnership Act 1932 **or** Partnership firm registered under Limited Liability Partnership Act 2008 or Proprietary firm with their registered office in India for the last three (3) years.	Copy of valid Certificate of Registration attested by Authorised signatory / Certificate of Incorporation		
2.	Power of Attorney in the name of authorized signatory authorizing him for signing the bid documents or related clarifications on bid documents **Or** Original Authorization in Letter Head in case of Partnership Firm **Or** Original Self Certificate in Letter Head in case of Proprietorship naming/ indicating the person authorized to sign the bid	Scanned copy of Original Power of Attorney letter in a Non-Judicial Stamp Paper of at-least Rs.100/- **or** Board Resolution in Letter Head in original in case of Registered Limited Companies **Or** Original Authorization in Letter Head in case of Partnership Firm **Or** Original Self Certificate in Letter Head in case of Proprietorship naming/ indicating the person authorized to sign the bid (PDF).		
3.	Certificate by authorized signatory confirming acceptance of all tender terms and conditions.	Copy of the certificate signed by the authorized signatory		

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no. where document occurs in the bid
4.	The bidder should be empanelled with CERT-In at the time of bid submission	Copy of empanelment letter signed by the authorized signatory		
5.	The bidder must have a positive net worth in any two (2) of the three (3) financial years (2020-21, 2021-22, and 2022-23).	Duly signed & stamped CA certificate for positive net worth.		
6.	The bidder must have a registration number for GSTN	Duly signed & stamped copies of relevant certificates of registration		
7.	Bidder must have a valid PAN	Duly signed & stamped copy of PAN card / certificate		
8.	The bidder must be a single legal entity/ individual organization. Consortium shall not be allowed.	Undertaking signed by authorized signatory		
9.	The bidder must have filed its Income Tax Returns for 3 financial years (2020-21, 2021-22,2022-23)	Duly signed and stamped copies of Income Tax Returns Digitally signed ITR may be provided		
10.	To confirm in Yes or No, whether the bidder falls under the Micro, Small and Medium Enterprises Development Act, 2006. Further, keep informed to NICSI whether there is any change of the status of the company.	If yes, duly signed & stamped copy of valid Certificate for similar service line as mentioned in the tender must be furnished. Mere registration as SSI Unit will not be acceptable.		
11.	The bidder must furnish its ISO 9001:2015 certificate and an ISO 27001: 2013 certificate	Bidder should submit copies of these certifications		
12.	Bidder must have an average annual turnover of **INR 10 Crore** or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 from application security services only.	The turnover certificate from application security services should duly certified by registered CA		

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no. where document occurs in the bid
13.	The bidder should have experience of at least **3 years** in providing Information Security Audit and consulting services as on the date of bid submission	Undertaking on letter head signed by authorized signatory as per **Annexure-12** certified by CA		
14.	The bidder must have executed a minimum of **fifteen (15)** major projects in last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (Central / State / PSUs) departments or private organizations with at least three or more projects executed in Government and at least ten executed in India. ***Note:** Each project value should be more than 3Lakh*	Provide duly signed & stamped documents, for each project as per **Annexure-8**		
15.	The organization should have at least **60** Information Security professional on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**		
16.	The bidder, as on the date of bid submission, has not been blacklisted or debarred by NICSI or any of the Central or State Government Organisation/ Public Sector Undertaking/ Autonomous Body etc.	An undertaking (self-certification in company's letterhead) is to be submitted as per format provided in **Annexure-10**.		

On behalf of [bidder's name]

Authorized Signature [In full and initials]:
Name & Title of signatory:
Name of Firm:
Address:
Seal/Stamp of bidder:
Place:
Date:

NOTE:

a) All bid documents must be clearly signed and stamped by the Authorized Signatory of the bidder.

b) Only those bidders, who satisfy the eligibility requirements and accept the terms and conditions of this RFP document without any pre-condition shall be short-listed for further technical evaluation.

ANNEXURE-5: TECHNICAL EVALUATION CRITERIA

S. No.	Criteria	Required Documents	Max Marks	Marks Obtained
1	Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- **5 Marks** • For each additional 2 Crores- **1 Mark**	The turnover certificate duly certified by registered CA	**10**	
2	No. of years in providing Information Security Audit and consulting services (Max Marks 5) • For 3 years in providing Information Security Audit and consulting services - **2 Marks** • For each additional 2 years- **1 Mark**	Declaration on letter head signed by authorized signatory as per **Annexure-12** certified by CA	**5**	
3	No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-**5 Marks** • For each additional 20 professionals- **1 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	
4	No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications) • For 20 Certified Professionals- **2 Marks** • For each additional 10 Certified Professionals- **1 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**5**	
5	No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors **– 4 Marks** • For each 10 additional senior auditors- **2 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	
6	No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors **– 4 Marks** • For each 10 additional Junior auditors- **2 Marks** Note: The names of the auditors on the senior and junior lists shouldn't match.	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	

7	No. of Projects executed in last 3 Financial Years i.e., FYs. 2020-21, 2021-22, 2022-23 • For 15 Projects- **5 Marks** • For each additional 5 Projects- **2 Marks**	Copy of relevant supporting documents as per **Annexure-8**	**12**	
8	• Experience in SAST (Static Application Security Testing) /Source Code Analysis testing across different development environments.	Copy of relevant documents, duly signed, and stamped from authorized signatory	**3**	
9	The organization should have at least 7 security assessment solutions including vulnerability assessment and application testing automated tools. • For 3 commercial licenses out of 7 security assessment solutions- **3 Marks** • For each additional commercial license- **1 Marks**	Copies of license agreements of commercial tools and copy of self-certified, duly signed and stamped from authorized signatory for open-source tools	**5**	
10	Presentation detailing the Approach & Methodology for carrying out the Security Audit related activity: • Approach & Methodology **(5 Marks)** • Proposed Work Plan, Test cases of large projects undertaken **(10 marks)** • Experience of Web Services/API/mobile testing **(10 marks)** • Experience of Data Security Audit, Application, and database Server compliance/ Hosting infrastructure testing **(5 marks)**	Copy of presentation may be submitted at the time of presentation	**30**	
	Total Marks		**100**	

Note: - *The same resource should not be shown for dual (i.e., both senior and junior auditor) category.*

- ✓ *The eligible bidder's (qualified in pre-qualification criteria as per Annexure-4) will be notified later regarding the technical presentation.*
- ✓ *The bidder who would score 70 % Marks or more will be termed technically qualified for further evaluation.*

ANNEXURE-6: ABRIDGED FINANCIAL BID

<To be submitted on the letterhead of the bidder>

Name of the Bidder:_____

Gross Total Value (X)	**Rs. ……. (In figures)**	**Rupees ……. (In words)**

(Reproduce value of GTV(X) as per the Annexure-7 – Detailed Financial Bid)

Note:

i. Prices should be quoted in Indian Rupee only and indicated in both figures and words. The amount mentioned in words will prevail.
ii. The bidder at first should calculate the value of GTV(X) in detailed financial bid.
iii. In this Performa, the GROSS TOTAL VALUE (X) as calculated in Detailed Financial Bid must be reproduced as above.
iv. This Performa shouldn't contain any detailed rates otherwise the bid will be rejected.

Date:

Place:

Authorized Signatory Name:

Signature:

Bidder Seal/Stamp:

ANNEXURE-7: DETAILED FINANCIAL BID

<To be submitted on the letterhead of the bidder>

A. Application Security Audit (Refer Annexure-13 for Categorization criteria)

S. No. (1)	Activities (2)	Static and Minimal Dynamic (INR) (3)	Dynamic (Medium) (INR) (4)	Dynamic (Big) (INR) (5)	Weightage (6)	Total Value(X1) (7) = Column ((3) +(4) + (5)) * (6)
1	Application Security Audit Services (Manual Audit) per web application/ API/ Services rate				5	
2	Application Security Audit Services (SAST + Manual Audit) per web application/API/Services rate				3	
3	APK/IoS Mobile App Audit (audit should also include number of webservices/APIs linked) rate				5	
Sum of Column (6) of Rows Sl. No. 1 to 3						**X1**

B. Penetration Testing and Comprehensive Security Assessment

<To be submitted on the letterhead of the bidder>

S. No. (1)	Activities (2)	Unit (Number of Websites/ Resource Name) (3)	Man-month Rates/ per website Audit/ PT Rates/ CSA per day rate (INR) (4)	Weightage (5)	Total Value(X2) (6) = Column (4) * (5)
1	Application Penetration Testing (PT) (External Testing) per Web application/API/Services /Mobile App rate	Less than 25		5	
		26 - 50			
		51 - 100			
		More than 100			
2	Application Penetration Testing (PT) (External and Internal Testing) per Web application/API/ Services/ Mobile App rate	Less than 25		3	
		26 - 50			
		51 – 100			
		More than 100			
3	Comprehensive Security Assessment (CSA) per day rate	NA		5	
4	Resources per man month rate	Senior Auditor		5	
		Junior Auditor		3	
Sum of Column (6) of Rows Sl. No. 1 to 4					**X2**

Grand Total Value (X)= X1+X2

Grand Total Value (X) in figure= Rs……

Grand Total Value (X) in Words = Rupees……

Important Note:

i. All fields in the financial bid format are MANDATORY.
ii. The Bidder's billing Location must be anywhere in India only.
iii. Prices must be quoted in Indian Rupees and indicated both in figures and words. Price in words will prevail, in the event of any mismatch.

iv. The Basic Cost, taxes as applicable and other levies must be quoted explicitly.

v. The audit means the completion of the entire audit cycle for a particular website till all the vulnerabilities are addressed.

vi. The Single web application Security Audit costing assessment would be decided based on the projected "Scope of Work" requirement and would be undertaken through bidding process based on audit resources man month rate from NICSI empanelled pool of security audit agencies.

vii. The Comprehensive Security Assessment (CSA) costing assessment would be decided based on (i) Technical evaluation of the projected "Scope of Work" requirement and would be undertaken through QCBS based bidding process (refer Annexure- 14 for details). (ii) The financial for CSA would be based on number of days projected as per the defined scope document. Only NICSI empanelled vendors fulfilling the criteria would be eligible in this bidding process.

The Evaluation Committee will select the Agency by giving 70% weightage to the concept and designs (technical evaluation) and 30% weight age on the price bid (financial evaluation).

viii. The empanelled bidder should pay a minimum of 65% of the quoted basic rate to the auditors. The appropriate proof in this respect such as a CTC (Cost to company) document should be provided to NIC/NICSI.

ix. The resources mentioned at S.no 6 should have the same minimum eligibility criteria as mentioned in 14. TECHNICAL SPECIFICATION for Application Security Audit and Compliance Services, point 3. Team Profile

x. For consideration of their bids, the bidders must quote for all the resource levels. The rates quoted should be as per industry standards for the prescribed experience. For any of the resource levels, bids quoting zero will be rejected and execution of Bid Securing Declaration.

Date:

Place:

Authorized Signatory Name:

Signature:

Bidder Seal/Stamp:

ANNEXURE-8: PROJECT/ASSIGNMENT DETAILS

S. No.	Details of Assignment	Details (reference Page No. of Bid Proposal)
1	Name of the Client & Category (Government/PSU/ Agency or Private Entity or others)	
2	Name of the Client's Contact person with phone number & email id	
3	Project/Assignment Name and summary (5 lines)	
4	Project/Assignment Start Date:	
5	Project/Assignment Completion Date:	
6	Total Project Cost (INR):	
7	No. of Resources deployed	
8	Enclosed relevant document(s) specifying the Scope of work, indicating Engagement value, Assignment's Profile and Assignment's discipline.	i. Copy of Completion Certificates received from the client, **OR** ii. Copy of Work Orders/LOI /Purchase orders/Contract + Self attested Phase Completion Certificate issued by the Statutory Auditor/CA/CS), **OR** iii. Copy of Work Order/LOI /Purchase orders/Contract +Project/Phase Completion Certificate received from Client

Note:
Kindly attach this filled in annexure assignment details as supporting document for establishing the eligibility and technical evaluation. This must be furnished with page numbers indicated in the index. Please use separate sheets wherever necessary.

Date:

Place:

Authorized Signatory Name:

Signature:

Bidder Seal/Stamp:

ANNEXURE-9: PERFORMA FOR NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

<To be submitted on the letterhead of the bidder>

WHEREAS, we the undersigned Service Provider, _____, having our principal place of business/ registered office at _____, are desirous of providing services under the terms and conditions as stipulated under Tender No. NICSI/ eGov Professionals/2020/11 dated <*dd-mm-yyyy*> "Empanelment of Consulting Organisation for e-Governance Project/Services in ICT Area" (hereinafter called the said 'RFP') to NICSI, having its office at HALL NO. 2&3, 6TH FLOOR, NBCC TOWER, 15 BHIKAJI CAMA PLACE, NEW DELHI – 110066., hereinafter referred to as 'Purchaser' and,

WHEREAS, the Service Provider is aware and confirms that the Purchaser's business/ operations, information, Application/software, hardware, business data, architecture schematics, designs, storage media and other information / documents made available by the Purchaser in the RFP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and/or proprietary to the Purchaser,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the Purchaser's grant to the Service Provider of specific access to Purchaser's confidential information, property, information systems, network, databases and other data, the Service Provider agrees to all of the following conditions.

It is hereby agreed as under:

1. The confidential information to be disclosed by the Purchaser under this Agreement ("Confidential Information") shall include without limitation, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to processes, methodologies, algorithms, risk matrices, thresholds, parameters, reports, deliverables, work products, specifications, architecture, project information, money laundering typologies, related computer programs, systems, trend analysis, risk plans, strategies and information communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site to which access is permitted by the Purchaser.
2. Confidential Information does not include information which:
    a. the Service Provider knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
    b. information in the public domain as a matter of law.
    c. is obtained by the Service Provider from a third party without any obligation of confidentiality.
    d. the Service Provider is required to disclose by order of a competent court or regulatory authority.

e. is released from confidentiality with the written consent of the Purchaser.

The Service Provider shall have the burden of proving hereinabove are applicable to the information in the possession of the Service Provider.

3. The Service Provider agrees to hold in trust any Confidential Information received by the Service Provider, as part of the Tendering process or otherwise, and the Service Provider shall maintain strict confidentiality in respect of such Confidential Information, and in no event a degree of confidentiality less than the Service Provider uses to protect its own confidential and proprietary information. The Service Provider also agrees:
    a. to maintain and use the Confidential Information only for the purposes of bidding for this RFP and thereafter only as expressly permitted herein.
    b. to only make copies as specifically authorized by the prior written consent of the Purchaser and with the same confidential or proprietary notices as may be printed or displayed on the original.
    c. to restrict access and disclosure of Confidential Information to their employees, agents, consortium members and representatives strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this clause; and
    d. to treat Confidential Information as confidential unless and until Purchaser expressly notifies the Service Provider of release of its obligations in relation to the said Confidential Information.
4. Notwithstanding the foregoing, the Service Provider acknowledges that the nature of activities to be performed as part of the Tendering process or thereafter may require the Service Provider's personnel to be present on premises of the Purchaser or may require the Service Provider's personnel to have access to software, hardware, computer networks, databases, documents, and storage media of the Purchaser while on or off premises of the Purchaser. It is understood that it would be impractical for the Purchaser to monitor all information made available to the Service Provider's personnel under such circumstances and to provide notice to the Service Provider of the confidentiality of all such information.

    Therefore, the Service Provider shall disclose or allow access to the Confidential Information only to those personnel of the Service Provider who need to know it for the proper performance of their duties in relation to this project, and then only to the extent reasonably necessary. The Service Provider will take appropriate steps to ensure that all personnel to whom access to the Confidential Information is given are aware of the Service Provider's confidentiality obligation. Further, the Service Provider shall procure that all personnel of the Service Provider are bound by confidentiality obligation in relation to all proprietary and Confidential Information received by them which is no less onerous than the confidentiality obligation under this agreement.
5. The Service Provider shall establish and maintain appropriate security measures to provide for the safe custody of the Confidential Information and to prevent unauthorised access to it.
6. The Service Provider agrees that upon termination/expiry of this Agreement or at any time during its currency, at the request of the Purchaser, the Service Provider shall promptly deliver to the Purchaser the Confidential Information and copies thereof in its

possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Service Provider or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

7. Confidential Information shall always remain the sole and exclusive property of the Purchaser. Upon completion of the Tendering process and/or termination of the contract or at any time during its currency, at the request of the Purchaser, the Service Provider shall promptly deliver to the Purchaser the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Service Provider or its Affiliates or directors, officers, employees or advisors based on the Confidential Information within a period of sixty days from the date of receipt of notice, or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of the Purchaser. Without prejudice to the above the Service Provider shall promptly certify to the Purchaser, due and complete destruction, and return. Nothing contained herein shall in any manner impair rights of the Purchaser in respect of the Confidential Information.
8. If the Service Provider hereto becomes legally compelled to disclose any Confidential Information, the Service Provider shall give sufficient notice and render best effort assistance to the Purchaser to enable the Purchaser to prevent or minimize to the extent possible, such disclosure. Service Provider shall not disclose to a third party any Confidential Information or the contents of this RFP without the prior written consent of the Purchaser. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Service Provider applies to its own similar Confidential Information but in no event less than reasonable care.

For and on behalf of:
(Service Provider)

Authorised Signatory:

Name:

Designation:

Office Seal:

Place:

Date:

ANNEXURE-10: DECLARATION-CUM-UNDERTAKING REGARDING BLACKLISTING/NON-BLACKLISTING BY NICSI

(Self-certification in company's letterhead)

I / We, Proprietor/ Partner(s) / Director(s) of M/S. _____ hereby declare that the firm/company namely M/s. _____, as on the date of bid submission, has not been blacklisted or debarred by NICSI or any of the Central or State Government Organisation/ Public Sector Undertaking / Autonomous Body etc.

In case the above information found false I/We are fully aware that the tender/ contract will be rejected/cancelled by NICSI and execution of Bid Securing Declaration. In addition to the above NICSI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

OR

I/We Proprietor/ Partner(s)/ Director(s) of M/s. _____ hereby declare that the firm/company namely M/S_____, was blacklisted or debarred by NICSI, or any other Central or State Government Organization/Public Sector Undertaking/Autonomous Body etc. for a period of _____ months/years w.e.f. _____. The period is over on _____ and, as on the date of bid submission the firm/company is not in active blacklisting period and now entitled to take part in Government tenders

In case the above information found false I/We are fully aware that the tender/ contract will be rejected/cancelled by NICSI and execution of Bid Securing Declaration. In addition to the above NICSI will not be responsible to pay the bills for any completed / partially completed work if Tender was allotted.

(Signature of Bidder with Seal)
Name:
Capacity in which as signed:
Name & address of the Company / Firm:
Date:
Place:

ANNEXURE-11: EMPLOYEES DETAIL UNDERTAKING

<On Company's Letter Head>

<Date>

To

The Managing Director,

NICSI, 1st Floor, NBCC Tower

Bhikaji Kama Place,

New Delhi

Sub: Undertaking for employees on company pay-roll for the past one years

Dear Sir,

This is to certify that <Mention Bidder's company Name> have_____ number of employees on company's payroll with minimum 1 years. The qualification and years of experience of mentioned number of employees complies with asked educational qualifications, experiences, and indicative work profile for the NICSI's tender no. _____.

S. No.	Employee Name	Designation	Educational Qualifications	Certifications (Such as CEH, CISSP, CISA, OSCP, or GIAC)	Years of Experiences	Total Years in Company's Payroll

Signature of HR Head:

Signature of Authorized Signatory:

Date & Stamp of Company:

Note:

1) Bidders must submit the list of the employees for mentioned profile as per details given in eligibility/technical criteria. NICSI may verify the genuineness on the sample basis up to the satisfaction, by asking the detailed CV and other details.

2) The proposed resources in Junior auditors Profile and senior auditors Profile should be different and mutually exclusive.

ANNEXURE-12: UNDERTAKING ON PREVIOUS EXPERIENCE

<On Company's Letter Head>

I / We, Proprietor/ Partner(s) / Director(s) of M/s. _____ hereby declare that the firm/company namely M/s. _____, with registration no. _____ dated _____ as on the date of bid submission, have _____ years of experiences in Application Security Audit and Compliance services.

In case the above information found false I/We are fully aware that the tender/ contract will be rejected/cancelled by NICSI and execution of Bid Securing Declaration. Also, the agency will be debarred for two years to participating in any tender published through NIC/NICSI. In addition to the above NICSI will not be responsible to pay the bills for any completed / partially completed work if tender was allotted.

(Signature of Bidder with Seal) (Certified by CA)

Name:

Capacity in which as signed:

Name & address of the Company / Firm:

Date:

Place:

ANNEXURE-13: CATEGORIZATION CRITERIA

1) Criteria for Categorizing Web Applications/Services/APIs

Static and minimal dynamic	Dynamic (medium)	Dynamic (Big)
<50 Entry Points OR <3 Roles in Authenticated Sites	>50 and <=250 Entry Points OR >=3 and <=7 Roles in Authenticated Sites	>250 Entry Points OR >7 Roles in Authenticated Sites

2) APK/IoS Mobile App Audit (audit should also include number of webservices/APIs linked). The Categorization (static and minimal dynamic/Dynamic(medium)/Dynamic (Big) of consolidated Entry points and Roles for all Web Services/APIs should follow the same criteria as mentioned in clause 1 above.
3) Payment Gateway linked applications would fall only under Dynamic (medium) or Dynamic (Big) as per clause 1 criteria mentioned above.

ANNEXURE-14: COMPREHENSIVE SECURITY ASSESSMENT FORMAT

(Sample Scope of Work format needed by External Auditing agency)

1. **External Facing Infrastructure Assessment**

Components	Quantity
Router	
Firewall	
IPS	
Switch(L3/L2)	
Load Balancers	
UTM	
WAF	
Public Facing IPs	

2. **Website Compliance assessments**

Components	Quantity
Web Applications/Web Services (with URLs)	
API	
Mobile Applications	

3. **Deployment and Network Architecture Review**

(Network Diagram depicting project deployment Architecture with details of IPs with Schema.)

4. **Internal Infrastructure Assessment**

Operating Systems of Servers	
Application Servers (Web Server, Development framework/ environment details)	
Databases	
VPN IPs	
Switch(L2)	

5. **Miscellaneous (Any Other Information such as Project documentation, workflow details for each application component, etc.)**

Note:

1) Comprehensive infrastructure assessment for all components should be project specific only.
2) The respective auditor may ask for additional requirements/documents from concerned project-coordinators. Use additional sheet as per the requirement.
3) It is just a suggestive sample template. It can be further modified as per the project requirement.

ANNEXURE-15: TECHNICAL COMPLIANCE SHEET FOR EVALUATION OF CSA BID

S. No.	Section	Criteria	Total Marks (100)	Documentary Evidence	Reference/ page enclosed in the bid
1	Presentation	Presentation detailing the Approach & Methodology for carrying out the said activity as per defined scope for CSA Approach & Methodology **(50 Marks)** Proposed Work Plan, Test cases of large projects undertaken **(20 marks)** Experience of Web Services/API/mobile testing **(15 marks)** Experience of Data Security Audit, Application, and database Server compliance/ Hosting infrastructure testing **(15 marks)**	100		

No. 10(21)/2022-NICSI

NATIONAL INFORMATICS CENTRE SERVICES INC. (NICSI)
(A Government of India Enterprise under NIC)
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Hall No. – 1st Floor, NBCC Tower
15, Bhikaiji Cama Place, New Delhi: - 110 066
Phone: 91-11-22900525/534/35 Fax: 91-11-26105212
Email: tender-nicsi@nic.in

Date: - 30.11.2023

Corrigendum-II (Modification of Clauses along with Pre-Bid Responses and Extension of Dates)

Tender No: NICSI/Application Security Audit/2023/05

Refer NICSI's open tender no. NICSI/Application Security Audit/2023/05 for Request for proposal for Empanelment of Agencies for Providing Application Security Audit and Compliance Services.

The last date for Bid Submission of tender has been extended upto 11.12.2023 till 15:00 Hours and the same will be opened on 12.12.2023 at 15:30 Hours.

The modification in the respective section of the RFP through this corrigendum is enclosed herewith. This corrigendum shall be read along with the published tender Document.

No. 10(21)/2022-NICSI
नेशनल इन्फार्मेटिक्स सेंटर सर्विसेजइंक.(निक्सी)
(गवर्नमेंटऑफ़ इंडिया एंटरप्राइज अंडर एनआईसी)
इलेक्ट्रॉनिक्सऔर सूचना प्रौद्योगिकी मंत्रालय
हॉल नंबर - पहली मंजिल एनबीसीसी टॉवर 15,
भीकाईजी कामा प्लेस, नईदिल्ली:-110066
टेलीफोन नंबर: 91-11-22900525/534/35
ईमेल :**tender-nicsi@nic.in**

दिनांक: - 30.11.2023

शुद्धिपत्र-II (खंडों में संशोधन के साथ बोली-पूर्व प्रतिक्रियाओं और तिथियों का विस्तार)

निविदा संख्या: निक्सी/ एप्लीकेशन सिक्योरिटी ऑडिट /2023/05

एनआईसीएसआई की खुली निविदा संख्या देखें। एनआईसीएसआई/एप्लिकेशन सुरक्षा ऑडिट/2023/05 एप्लिकेशन सुरक्षा ऑडिट और अनुपालन सेवाएं प्रदान करने के लिए एजेंसियों के पैनल में शामिल करने के प्रस्ताव के लिए अनुरोध के लिए।

बोली जमा करने की अंतिम तिथि 11.12.2023 को 15:00 बजे तक बढ़ा दी गई है और इसे 12.12.2023 को 15:30 बजे खोला जाएगा।

इस शुद्धिपत्र के माध्यम से आरएफपी के संबंधित अनुभाग में संशोधन इसके साथ संलग्न है। यह शुद्धिपत्र प्रकाशित निविदा दस्तावेज़ के साथ पढ़ा जाएगा।

S. No.	Section	Clause	Reference Page No.	Existing Clause/Section	Modified Clause/Section
1	1 Fact Sheet	Vendor Panel Size	5	Up to 5(Five) Vendors	All bidders scoring 70% marks in Technical Evaluation Criteria (Annexure-5) **and whose bids are within range of 30% of average Grand Total Value (GTV)**
2	4 Scope of Work	Scope of Work	8	NICSI as part of the Application Security Audit and Compliance Services will empanel maximum of five agencies for the execution of work.	NICSI as part of the Application Security Audit and Compliance Services will empanel all bidders scoring 70% marks in Technical Evaluation Criteria (Annexure-5) **and whose bids are within range of 30% of average Grand Total Value (GTV)** for the execution of work
3	Section 4.3	COMPREHENSIVE SECURITY ASSESSMENT	12	**COMPREHENSIVE SECURITY ASSESSMENT** The comprehensive infrastructure assessment is to preview the required "scope of work" outlined for respective NIC/NICSI projects which apart from audit of complete Deployment architecture plan and workflow of hosted applications, also includes compliance security testing of all in-line network devices, network security devices, operating systems, Web Servers, Hosting frameworks, Business Logic compliance and Data Security control checks, Mobile Apps, Malware analysis, Forensic analysis, UIDAI compliance requirements, APIs and databases related with that NIC/NICSI project requirement.	**COMPREHENSIVE SECURITY ASSESSMENT (CSA)** The comprehensive infrastructure assessment is to preview the required "scope of work" outlined for respective NIC/NICSI projects which apart from audit of complete Deployment architecture plan and workflow of hosted applications, also includes compliance security testing of all in-line network devices, network security devices, operating systems, Web Servers, Hosting frameworks, Business Logic compliance and Data Security control checks, Mobile Apps, Malware analysis, Forensic analysis, UIDAI compliance

S. No.	Section	Clause	Reference Page No.	Existing Clause/Section	Modified Clause/Section
				Security Audit through CSA activity should be taken up as per the outlined scope and emphasise on the broader and granular coverage of critical ICT NIC/NICSI projects. The audit process shall adhere to a well-defined checklist document as per the defined scope of CSA requirement.	requirements, APIs and databases related with that NIC/NICSI project requirement. Security Audit through CSA activity should be taken up as per the outlined scope and emphasis on the broader and granular coverage of critical ICT NIC/NICSI projects. The audit process shall adhere to a well-defined checklist document as per the defined scope of CSA requirement. **In the similar way a defined scope for seeking "Patching as a Service support" can also be planned and sought by the concerned user department/ministry.**
4	9. EMPANELMENT	9.1 Signing of Contract	26	b. NICSI will have a panel of vendor up to 5 (Five) empaneled vendors	b. NICSI will have a panel empaneled vendors of all bidders scoring 70% marks in Technical Evaluation Criteria (Annexure-5) **and whose bids are within range of 30% of average Grand Total Value (GTV)**
5	9. EMPANELMENT	9.1 Signing of Contract	26	d. The rates finalized shall remain valid during empanelment/extended empanelment.	d. The rates finalized shall remain valid for initial 2 Years. In 3rd Year 7% increase in rates shall be done. If, the empanelment is extended, rates shall be further increased at 7% for 4th & 5th year.
6	9. EMPANELMENT	9.1 Signing of Contract	27	Additional Clause	p. The empaneled vendors should remain empaneled with CERT-In throughout the

<table>
<tr><th>S. No.</th><th>Section</th><th>Clause</th><th>Reference Page No.</th><th>Existing Clause/Section</th><th>Modified Clause/Section</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>NICSI empanelment period.</td></tr>
<tr><td>7</td><td>9.2 SECURITY DEPOSIT FOR EMPANELMENT</td><td>SECURITY DEPOSIT FOR EMPANELMENT</td><td>27</td><td>b. The Security Deposit for this category is mentioned as under:<table><tr><th>Security Deposit Amount</th><th>Security Deposit Amount (words)</th></tr><tr><td>INR 25 Lakhs</td><td>Rupees Twenty-Five Lakh</td></tr></table></td><td>b. The Security Deposit for this category is mentioned as under:<table><tr><th>Security Deposit Amount</th><th>Security Deposit Amount (words)</th></tr><tr><td>INR 15 Lakhs</td><td>Rupees Fifteen Lakh</td></tr></table></td></tr>
<tr><td>8</td><td>Annexure-4</td><td>ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)</td><td>51</td><td>Annexure-4</td><td>Please refer revised Annexure - 4 in this Corrigendum</td></tr>
<tr><td>9</td><td>Annexure-5</td><td>TECHNICAL EVALUATION CRITERIA</td><td>55</td><td>Annexure-5</td><td>Please refer revised Annexure - 5 in this Corrigendum</td></tr>
<tr><td>10</td><td>Annexure-8: PROJECT/ ASSIGNMENT DETAILS</td><td>Sr. No. 8</td><td>61</td><td>i. Copy of Completion Certificates received from the client,
OR
ii. Copy of Work Orders/LOI /Purchase orders/Contract + Self attested Phase Completion Certificate issued by the Statutory Auditor/CA/CS),
OR
iii. Copy of Work Order/LOI /Purchase orders/Contract +Project/Phase Completion Certificate received from Client</td><td>i. Copy of Work Orders/LOI /Purchase orders/Contract + Completion Certificates received from the client,
OR
ii. Copy of Work Order/LOI /Purchase orders/Contract +Project/Phase Completion Certificate received from Client
OR
iii. Copy of Work Orders/LOI /Purchase orders/Contract + Self attested Phase Completion Certificate issued by the Statutory Auditor/CA/CS)</td></tr>
</table>

ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)

This states the eligibility criteria essential for qualifying as a prospective bidder for this tender.

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no.
1.	The bidder should be a company registered in India under the relevant act such as Companies Act 1956/ 2013, or a partnership registered under the India Partnership Act 1932 or Partnership firm registered under Limited Liability Partnership Act 2008 or Proprietary firm with their registered office in India for the last three (3) years.	Copy of valid Certificate of Registration attested by Authorised signatory / Certificate of Incorporation		
2.	Power of Attorney in the name of authorized signatory authorizing him for signing the bid documents or related clarifications on bid documents Or Original Authorization in Letter Head in case of Partnership Firm Or Original Self Certificate in Letter Head in case of Proprietorship naming/ indicating the person authorized to sign the bid	Scanned copy of Original Power of Attorney letter in a Non-Judicial Stamp Paper of at-least Rs.100/- or Board Resolution in Letter Head in original in case of Registered Limited Companies Or Original Authorization in Letter Head in case of Partnership Firm Or Original Self Certificate in Letter Head in case of Proprietorship naming/ indicating the person authorized to sign the bid (PDF).		
3.	Certificate by authorized signatory confirming acceptance of all tender terms and conditions.	Copy of the certificate signed by the authorized signatory		
4.	The bidder should be empanelled with CERT-In at the time of bid submission	Copy of empanelment letter signed by the authorized signatory		
5.	The bidder must have a positive net worth in any two (2) of the three (3) financial years (2020-21, 2021-22, and 2022-23).	Duly signed & stamped CA certificate for positive net worth.		

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no.
6.	The bidder must have a registration number for GSTN	Duly signed & stamped copies of relevant certificates of registration		
7.	Bidder must have a valid PAN	Duly signed & stamped copy of PAN card / certificate		
8.	The bidder must be a single legal entity/ individual organization. Consortium shall not be allowed.	Undertaking signed by authorized signatory		
9.	The bidder must have filed its Income Tax Returns for 3 financial years (2020-21, 2021-22,2022-23)	Duly signed and stamped copies of Income Tax Returns Digitally signed ITR may be provided		
10.	To confirm in Yes or No, whether the bidder falls under the Micro, Small and Medium Enterprises Development Act, 2006. Further, keep informed to NICSI whether there is any change of the status of the company.	If yes, duly signed & stamped copy of valid Certificate for similar service line as mentioned in the tender must be furnished. Mere registration as SSI Unit will not be acceptable.		
11.	The bidder must furnish its ISO 9001:2015 certificate and an ISO 27001: 2013 certificate	Bidder should submit copies of these certifications		
12.	Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 from application security services or Information Security Auditing Services.	The turnover certificate from application security services should duly certified by registered CA		
13.	The bidder should have experience of at least 3 years in providing Information Security Audit and consulting services as on the date of bid submission	Undertaking as per Annexure-12 signed by authorized signatory and certified by CA		
14.	The bidder must have executed a minimum of fifteen (15) major projects in last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (Central / State / PSUs) departments or private organizations with at least three or more	Provide duly signed & stamped documents, for each project as per Annexure-8		

S. No.	Criteria	Documents to be submitted as qualifying documents (100% Compliance)	Eligible (Yes/No)	Reference of enclosed proof along with page no.
	projects executed in Government and at least ten executed in India. *Note: Each project value should be more than 3 Lakh*			
15.	The organization should have at least 60 Information Security professional on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, ISO 27001 LA/LI or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.	Declaration on letterhead by HR head, counter-signed by authorized signatory as per Annexure-11		
16.	The bidder, as on the date of bid submission, has not been blacklisted or debarred by NICSI or any of the Central or State Government Organisation/ Public Sector Undertaking/ Autonomous Body etc.	An undertaking (self-certification in company's letterhead) is to be submitted as per format provided in Annexure-10.		

On behalf of [bidder's name]
Authorized Signature [In full and initials]:
Name & Title of signatory:
Name of Firm:
Address:
Seal/Stamp of bidder:
Place:
Date:

NOTE:

a) All bid documents must be clearly signed and stamped by the Authorized Signatory of the bidder.

b) Only those bidders, who satisfy the eligibility requirements and accept the terms and conditions of this RFP document without any pre-condition shall be short-listed for further technical evaluation.

ANNEXURE-5: TECHNICAL EVALUATION CRITERIA

S. No.	Criteria	Required Documents	Max Marks	Marks Obtained
1	Average annual turnover from application security / Information Security Auditing Services during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- **5 Marks** • For each additional 2 Crores- **1 Mark**	The turnover certificate duly certified by registered CA	**10**	
2	No. of years in providing Information Security Audit and consulting services (Max Marks 5) • For 3 years in providing Information Security Audit and consulting services - **2 Marks** • For each additional 2 years- **1 Mark**	Declaration on letter head signed by authorized signatory as per **Annexure-12** certified by CA	**5**	
3	No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-**5 Marks** • For each additional 20 professionals- **1 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	
4	No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/GIAC/ ISO 27001 LA/LI certifications) • For 20 Certified Professionals- **2 Marks** • For each additional 05 Certified Professionals- **1 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**5**	
5	No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC/ISO 27001 LA/LI certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – **4 Marks** • For each 05 additional senior auditors- **2 Marks**	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	
6	No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC/ ISO 27001 LA/LI certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – **4 Marks** • For each 05 additional Junior auditors- **2 Marks** Note: The names of the auditors on the senior and junior lists shouldn't match.	Declaration on letterhead by HR head, counter-signed by authorized signatory as per **Annexure-11**	**10**	
7	No. of Projects executed in last 3 Financial Years i.e., FYs. 2020-21, 2021-22, 2022-23 • For 15 Projects- **6 Marks** • For each additional 5 Projects- **2 Marks**	Copy of relevant supporting documents as per **Annexure-8**	**12**	

S. No.	Criteria	Required Documents	Max Marks	Marks Obtained
8	Experience in SAST (Static Application Security Testing) /Source Code Analysis testing across different development environments.	Copy of relevant documents, duly signed, and stamped from authorized signatory	**3**	
9	The organization should have at least 7 security assessment solutions including vulnerability assessment and application testing automated tools. • For 3 commercial licenses out of 7 security assessment solutions- **3 Marks** • For each additional commercial license- **1 Marks**	Copies of license agreements of commercial tools and copy of self-certified, duly signed and stamped from authorized signatory for open-source tools	**5**	
10	Presentation detailing the Approach & Methodology for carrying out the Security Audit related activity: • Approach & Methodology **(5 Marks)** • Proposed Work Plan, Test cases of large projects undertaken **(10 marks)** • Experience of Web Services/API/mobile testing **(10 marks)** • Experience of Data Security Audit, Application, and database Server compliance/ Hosting infrastructure testing **(5 marks)**	Copy of presentation may be submitted at the time of presentation	**30**	
	Total Marks		**100**	

Note: - *The same resource should not be shown for dual (i.e., both senior and junior auditor) category.*

- ✓ *The eligible bidder's (qualified in pre-qualification criteria as per Annexure-4) will be notified later regarding the technical presentation.*
- ✓ *The bidder who would score 70 % Marks or more will be termed technically qualified for further evaluation.*

Annexure-B

Pre-Bid Responses for TENDER NO. NICSI/Application Security Audit/2023/05
"Request for proposal for Empanelment of Agencies for Providing Application Security Audit and Compliance Services"

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
1	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	53	14. The bidder must have executed a minimum of fifteen (15) major projects in last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (Central / State / PSUs) departments or private organizations with at least three or more projects executed in Government and at least ten executed in India.	Request that you to modify the clause to below: The bidder must have executed a minimum of fifteen (15) major projects in the last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (iv) IS Audit/ Security Audit (V) VAPT (Central / State / PSUs) departments or private organizations with at least three or more projects executed in Government/PSU Sector.	No Change
2	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	53	15. The organization should have at least 60 Information Security professional on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.	We are an MSME certified organization with a certified workforce in all major security certifications as mentioned in the RFP with vast experience in catering to large PSUs/GOVT institutions/PSB in India. Request you to modify the existing clause to below: The organization should have at least 60 Information Security professionals on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, ISO 27001 LA/LI, CISM or GIAC and at least 5 should have two or more certificates at the time of bid submission.	Please refer to corrigendum
3	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	4. No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications) • For 20 Certified Professionals- 2 Marks	Request that you to modify the clause to below: No. of Certified Professionals (such as ISO 27001/CISM/CEH/ CISSP/ CISA/ OSCP/ GIAC certifications)	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			• For each additional 10 Certified Professionals- 1 Marks	• For 20 Certified Professionals- 2 Marks • For each additional 10 Certified Professionals- 1 Marks	
4	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	5. No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	Request that you to modify the clause to below: No. of Senior Application Security Auditors with 4+ Years of Experience with ISO 27001/CISM/CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	Please refer to corrigendum
5	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	6. No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors- 2 Marks Note: The names of the auditors on the senior and junior lists shouldn't match.	Request that you to modify the clause to below: No. of Junior Application Security Auditors with 1+ Years of Experience with ISO 27001/CISM/CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors- 2 Marks Note: The names of the auditors on the senior and junior lists shouldn't match.	Please refer to corrigendum
6	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	1. Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	Request that you to modify the clause to below: Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 10 Marks • For each additional 2 Crores- 2 Mark Total marks - 20 Mark	No Change
7	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA		3. No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-5 Marks • For each additional 20 professionals- 1 Marks	Request that you to modify the clause to below: No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-5 Marks • For each additional 5 professionals- 1 Marks	No Change

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
8	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	4. No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications) • For 20 Certified Professionals- 2 Marks • For each additional 10 Certified Professionals- 1 Marks	Request that you to modify the clause to below: No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications) • For 10 Certified Professionals- 2 Marks • For each additional 5 Certified Professionals- 1 Marks	Please refer to corrigendum
9	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	5. No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	Request that you to modify the clause to below: No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 10 Senior Auditors – 2 Marks • For each 5 additional senior auditors- 1 Marks Total Mark - 5 Marks	Please refer to corrigendum
10	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	6. No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors- 2 Marks Note: The names of the auditors on the senior and junior lists shouldn't match.	Request that you to modify the clause to below: No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 10 Junior Auditors – 2 Marks • For each 5 additional Junior auditors- 1 Marks Note: The names of the auditors on the senior and junior lists shouldn't match. Total Marks - 5 Marks	Please refer to corrigendum
11	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	56	7. No. of Projects executed in last 3 Financial Years i.e., FYs. 2020-21, 2021-22, 2022-23 • For 15 Projects- 5 Marks • For each additional 5 Projects- 2 Marks	Request that you to modify the clause to below: No. of Projects executed in last 3 Financial Years i.e., FYs. 2020-21, 2021-22, 2022-23 • For 10 Projects- 6 Marks • For each additional 2 Projects- 2 Marks Total Marks - 12	No Change

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
12	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	56	The same resource should not be shown for dual (i.e., both senior and junior auditor) category. ✓ The eligible bidder's (qualified in pre-qualification criteria as per Annexure-4) will be notified later regarding the technical presentation. ✓ The bidder who would score 70 % Marks or more will be termed technically qualified for further evaluation.	Request that you to modify the clause to below: The same resource should not be shown for dual (i.e., both senior and junior auditor) category. ✓ The eligible bidder's (qualified in pre-qualification criteria as per Annexure-4) will be notified later regarding the technical presentation. ✓ The bidder who would score 60 % Marks for MSME or more will be termed technically qualified for further evaluation.	No Change
13	Tender Notice & RFP Factsheet	5	Pre-bid meeting on 25.10.2023 at 11:30 Hrs. through Video Conference	It is mentioned in tender notice that pre-bid meeting will be held at NICSI HQrs New Delhi However in RFP it is mentioned that pre-bid meeting through Video Conference. Please clarify	No Change
14	9.1 Signing of Contract	26, point d	The rates finalized shall remain valid during empanelment/extended empanelment.	Since the empanelment will be for five years including extension. We request increment in rates from 7% to 10% per year subject to satisfactory performance of the empaneled auditor.	Please refer to corrigendum
15	9.3 Performance Bank Guarantee (PBG)	28, point a	The selected Service Provider shall be required to furnish a Performance Bank Guarantee (PBG) equivalent to 3% (Three Percent) of the Work Order/Purchase Order value.	There can be a case where work order value is less than 1 Lakh. In this case, PBG value shall be less than INR 3000 however bank charges for PBG can be more than PBG Value. Therefore, we request to waived off PBG for those work orders where value is less than 1 Lakh since our security despoit will also be submitted to NICSI during the empanelment	No Change
16	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PREQUALIFICATION)	52, point 4	The bidder should be empanelled with CERT-In at the time of bid submission	We request to modify the clause "The bidder should be empanelled with CERT-In since last 5 years"	No Change
17	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PREQUALIFICATION)	52, point 4	The bidder should be empanelled with CERT-In at the time of bid submission	We request to add this clause in RFP "The bidder should remain empanelled with CERT-In throughout the NICSI empanelment period"	Please refer to corrigendum
18	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PREQUALIFICATION)	52, point 12	Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 from application	There are many cases where work orders issued are for various security services including Application, Network, compliance etc. Since, this RFP scope also includes various services including Application, Comprehensive Security assessment (in-line network devices, operating systems, Web Servers, UIDAI	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			security services only.	compliance etc).Therefore, we request to replace "application security services" with "Information Security Auditing Services"	
19	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PREQUALIFICATION)	53, point 14	The bidder must have executed a minimum of fifteen (15) major projects in last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (Central / State / PSUs) departments or private organizations with at least three or more projects executed in Government and at least ten executed in India. Note: Each project value should be more than 3Lakh	We assume these 15 major projects in last 3 years may include any of the three mentioned categories. Please confirm	Yes
20	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PREQUALIFICATION)	53, point 15	The organization should have at least 60 Information Security professional on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.	Kindly add ISO 27001 certification as RFP scope also includes compliance services including UIDAI compliance etc. Also, we request you to remove para "at least 10 should have two or more certificates" as auditor with one certificate is very much capable to carry out the audit.	Please refer to corrigendum
21	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 1	Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	Request for following changes: * Average annual turnover from "**Information Security Auditing Services**" in place of "Application security" *For each additional 2 Crores - 1 Mark" may please be relaxed to "**1 Crore** - 1 Mark"	Please refer to corrigendum
22	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 3	No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-5 Marks • For each additional 20 professionals- 1 Marks	*For each additional 20 professionals - 1 Mark" may please be modified to "For each additional **10 professionals** - 1 Mark"	No Change
23	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 4	No. of Certified Professionals (such as CEH/CISSP/ CISA/ OSCP/ GIAC certifications) • For 20 Certified Professionals- 2 Marks	Kindly add ISO 27001 certification as RFP scope also includes compliance services including UIDAI compliance etc.	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			• For each additional 10 Certified Professionals- 1 Marks		
24	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 5	No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	Request for following changes: * Experience of 4+ Years of Experience may be modified to "**3+years of experience**" * Kindly add ISO 27001 certification as RFP scope also includes compliance services including UIDAI compliance etc. *For each 10 additional senior auditors- 2 Marks" may please be modifed to "For each **5 additional senior auditors**- 2 Marks"	No Change
25	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 6	No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors- 2 Marks	Request for following changes: * Kindly add ISO 27001 certification as RFP scope also includes compliance services including UIDAI compliance etc. *For each 10 additional junior auditors- 2 Marks" may please be modified to "For each **5 additional Junior auditors**- 2 Marks"	Please refer to corrigendum
26	Annexure 5: TECHNICAL EVALUATION CRITERIA	55, point 9	The organization should have at least 7 security assessment solutions including vulnerability assessment and application testing automated tools. • For 3 commercial licenses out of 7 security assessment solutions- 3 Marks • For each additional commercial license- 1 Marks	We request to modify "For each additional commercial license- 1 Marks" with **"For each additional commercial license- 2 Marks"**	No Change
27	Annexure 7: DETAILED FINANCIAL BID	60, point viii.	The empanelled bidder should pay a minimum of 65% of the quoted basic rate to the auditors. The appropriate proof in this respect such as a CTC (Cost to company) document should be provided to NIC/NICSI.	It is to inform you that there are various contributions which any Organisation do for employees and bear those expenses which are mentioned below: • Provident Fund (PF) • Gratuity • Leave Travel Allowance (LTA) • Insurance • Local Travel expenses • Expenses towards employee welfare (Annual	No Change

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
				functions etc.) • Cost for hiring through recruitment agency • Logistics requirements including laptops, tools etc. We request you to kindly remove the minimum pay clause.	
28	ANNEXURE-8: PROJECT/ASSIGNMENT DETAILS	61, point no. 8	Copy of Work Orders/LOI/Purchase orders/Contract+ Self attested Phase Completion Certificate issued by the Statutory Auditor/CA/CS)	We request to allow submit Copy of work orders + Self attested completion certificate from Bidder. Completion Certificate issued by the Statutory Auditor/CA/CS may please be removed	Please refer to corrigendum
29	Point 4 - Section - Scope of Work	RFP Page No. 8	In-Scope Location: The successful bidders must execute the activities at the following locations: • Regional Centre of Excellence AppSec Centres at Lucknow, Guwahati, Bhubaneshwar, Jaipur, and Thiruvananthapuram	Does the selected agency have to deploy resources in the Regional Centre of Excellence AppSec Centres at Lucknow, Guwahati, Bhubaneshwar, Jaipur, and Thiruvananthapuram.	Yes, as and when required by the user
30	Point 9 - Section - Empanelment - Sub-Section - Security Deposit for Empanelment Sub point 9.2 (b).	RFP Page No. 27	Security Deposit of INR 25 Lakhs	Request to consider and reduce the security deposit to 10 Lakhs.	Please refer to corrigendum
31	Annexure 4 - Eligibility Compliance Sheet (Pre-Qualification Sheet) -Point No 12	RFP Page No. 52	Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 from application security services only	Request to consider the turnover from Information Security Audit services instead of restricting to only application security services.	Please refer to corrigendum
32	Annexure 5 - Technical Evaluation Criteria Point No 1	RFP Page No. 55	Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	Request to consider the turnover from Information Security Audit services instead of restricting to only application security services.	Please refer to corrigendum
33	Annexure 5 - Technical Evaluation Criteria Point No 4	RFP Page No. 55	No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications) • For 20 Certified Professionals- 2 Marks	Request to include ISO 27001 certification also as UIDAI compliance requirements is a part of Comprehensive Security assessment as per the Scope of Work	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			• For each additional 10 Certified Professionals- 1 Marks		
34	Annexure 5 - Technical Evaluation Criteria Point No 5	RFP Page No. 55	No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years	Request to include ISO 27001 certification also as UIDAI compliance requirements is a part of Comprehensive Security assessment as per the Scope of Work	Please refer to corrigendum
35	Annexure 5 - Technical Evaluation Criteria Point No 5	RFP Page No. 55	No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For each 10 additional senior auditors- 2 Marks	Request to consider 2 Marks for each additional 5 Senior auditors instead of 10 additional Senior Auditors.	Please refer to corrigendum
36	Annexure 6 - Technical Evaluation Criteria Point No 6	RFP Page No. 55	No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years	Request to include ISO 27001 certification also as UIDAI compliance requirements is a part of Comprehensive Security assessment as per the Scope of Work	Please refer to corrigendum
37	Detailed Financial Bid - ANNEXURE – 7	3	Point viii. The empanelled bidder should pay a minimum of 65% of the quoted basic rate to the auditors. The appropriate proof in this respect such as a CTC (Cost to company) document should be provided to NIC/NICSI.	CTC includes laptops, mobile, conveyance, tools etc for which submitting proof is difficult. Hence, we request you to delete this clause.	No Change
38	1 FACTSHEET- Vendor Panel	5	Size- Up to 5(Five) Vendors	The scope envisaged in this RFP is huge for which 5 vendors may be insufficient. Hence, we recommend that if there are more than 5 technically qualified bidders, all of them should be empanelled	Please refer to corrigendum
39	8.2 FINANCIAL EVALUATION	25	Point P- Bids of those bidders whose Financial Bid's Gross Total Value (GTV) have a deviation beyond 30% (thirty Percent) on either side from the Average GTV of all the technically qualified bidders would be disqualified.	We request you to delete this clause and allow all bidders to match the L1 price. Those bidders who matches L1 price can be empanelled.	No Change

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
40	9.3 PERFORMANCE BANK GUARANTEE (PBG)	28	PERFORMANCE BANK GUARANTEE (PBG)	We request you to consider submission of Bank Guarantee for Man Power Mode only and not for Project Mode considering the fact that there is no time limit from Department to complete the project under Project Mode within a certain time line and the amount may not be huge. The administrative hassle increases because of small amount. Moreover, we are already giving Security Deposit at the time of empanelment.	No Change
41	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	52	Point 4 - The bidder should be empanelled with CERT-In at the time of bid submission	As this RFP is for 3 years plus additional 2 years extension option, therefore continuity of empanelment with CERT-In is necessary which proves the capability of the bidder. Hence, we recommend that this clause may be modified as under: **The bidder should be empanelled with CERT-In for continuously last 5 years**	Please refer to corrigendum
42	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	52	Point 12 - Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 from application security services only.	Application Security Services includes various services is mentioned in this RFP. Hence, we recommend that clause may be modified that the turnover of Rs. 10 Cr should be from IS Audit / Information Security Services as under: "Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-23 **from IS Audit / Information Security Services** .	Please refer to corrigendum
43	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	53	Point 13 - The bidder should have experience of at least 3 years in providing Information Security Audit and consulting services as on the date of bid submission - Undertaking on letter head signed by authorized signatory as per Annexure-12 certified by CA	A Chartered Accountant normally does not certify document printed on letter head of client. Hence, we recommend, that "Certified by CA" should be removed	Please refer to corrigendum
44	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	53	Point 15 - The organization should have at least 60 Information Security professional on their payroll for the last 1	We recommend to add other Certifications such as ISO 27001	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.		
45	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION)	53	Point 15 - The organization should have at least 60 Information Security professional on their payroll for the last 1 year. Out of 60 professionals, at least 20 should be certified in security, such as CEH, CISSP, CISA, OSCP, or GIAC, and at least 10 should have two or more certificates. at the time of bid submission.	Since the list of sufficent cerified professionals is furnished, we feel that there is no requirement that professionals should have two or more certificates. Hence, we recommend to delete the sentence "and at least 10 should have two or more certificates"	No Change
46	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr.Nos 1 - Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	Application Security Services includes various services is mentioned in this RFP. Hence, we recommend that clause may be modified that the turnover should be from "IS Audit / Information Security Services" instead of Application Security Services	Please refer to corrigendum
47	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr.Nos 1 - Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	We feel that the additional turnover required is very high since the bidder is already having a turnover of Rs. 10 Crores. Hence, we recommend the changes as under: "**For each additional 1 Crores it should be 1 mark**"	No Change
48	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr. Nos 3 - No. of Security Professionals in the payroll of firm from last 1 years. • For 60 Professionals-5 Marks • For each additional 20 professionals- 1 Marks	We feel that the additional professionals required is very high since the bidder is already having 60 Professionals. Hence, we recommend the changes as under: "**For each additional 10 Professionals it should be 1 mark**"	No Change
49	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr. Nos - 4 - No. of Certified Professionals (such as CEH/ CISSP/ CISA/ OSCP/ GIAC certifications)	We recommend to add other Certifications such as ISO 27001	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			• For 20 Certified Professionals- 2 Marks • For each additional 10 Certified Professionals- 1 Marks		
50	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr. Nos 5 - No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	We recommend to add other Certifications such as ISO 27001	Please refer to corrigendum
51	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr. Nos 5 - No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	We feel that the additional senior auditors required is very high since the bidder is already having 20 Senior Auditors. Hence, we recommend the changes as under: "**For each additional 5 Senior Auditors it should be 2 marks**"	Please refer to corrigendum
52	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr. Nos 5 - No. of Senior Application Security Auditors with 4+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Senior Auditors – 4 Marks • For each 10 additional senior auditors- 2 Marks	We recommend that the experience for senior auditor should be changed to 3+ Years from 4+ Years	No Change
53	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr.Nos 6 - No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors-	We recommend to add other Certifications such as ISO 27001	Please refer to corrigendum

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
			2 Marks Note: The names of the auditors on the senior and junior lists shouldn't match.		
54	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA	55	Sr.Nos 6 - No. of Junior Application Security Auditors with 1+ Years of Experience with CEH/CISSP/CISA/OSCP/GIAC certifications on organization's payroll from last 1 Years • For 20 Junior Auditors – 4 Marks • For each 10 additional Junior auditors- 2 Marks Note: The names of the auditors on the senior and junior lists shouldn't match.	We feel that the additional junior auditors required is very high since the bidder is already having 20 junior Auditors. Hence, we recommend the changes as under: "**For each additional 5 Junior Auditors it should be 2 marks**"	Please refer to corrigendum
55			Conflict of Interest	NIC is already empanelling Cyber Security Professionals CISOs for which RFP has already been floated. Since there would be conflict of interest for the same bidder giving CISO and also Auditing Services as per this RFP, We recommend that the organisations empanelled as Cyber Security Professionals CISOs as per above referred RFP will not be empanelled under this RFP for Providing Application Security Audit and Compliance Services being Conflict of Interest	No Change

No. 10(21)/2022-NICSI
NATIONAL INFORMATICS CENTRE SERVICES INC. (NICSI)
(A Government of India Enterprise under NIC)
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Hall No. – 1st Floor, NBCC Tower
15, Bhikaiji Cama Place, New Delhi: - 110 066
Phone: 91-11-22900525/534/35 Fax: 91-11-26105212
Email: tender-nicsi@nic.in

Date:- 09.01.2024

Corrigendum-VI (Extension Of Dates, Modification of Clauses and Reply of Queries)

Tender No: NICSI/Application Security Audit/2023/05

Refer NICSI's open tender no. NICSI/Application Security Audit/2023/05 for Request for proposal for Empanelment of Agencies for Providing Application Security Audit and Compliance Services.

1. The last date for Bid Submission of tender has been extended upto 18.01.2024 till 15:00 Hours and the same will be opened on 19.01.2024 at 15:30 Hours.

2. The modification in respective sections of the RFP through this corrigendum is enclosed herewith and this corrigendum shall be read along with the published tender document (Annexure-A).

3. Reply of Queries attached herewith (Annexure-B).

No. 10(21)/2022-NICSI
नेशनल इन्फार्मेटिक्स सेंटर सर्विसेजइंक.(निक्सी)
(गवर्नमेंटऑफ़ इंडिया एंटरप्राइज अंडर एनआईसी)
इलेक्ट्रॉनिक्सऔर सूचना प्रौद्योगिकी मंत्रालय
हॉल नंबर - पहली मंजिल एनबीसीसी टॉवर 15,भीकाईजी कामा प्लेस, नईदिल्ली:-110066
टेलीफोन नंबर: 91-11-22900525/534/35
ईमेल :**tender-nicsi@nic.in**

दिनांक: - 09.01.2024

शुद्धिपत्र-VI (तिथियों का विस्तार, खंडों में संशोधन और प्रश्नों का उत्तर)

निविदा संख्या: निक्सी/ एप्लीकेशन सिक्योरिटी ऑडिट /2023/05

एनआईसीएसआई की खुली निविदा संख्या देखें। एनआईसीएसआई/एप्लिकेशन सुरक्षा ऑडिट/2023/05 एप्लिकेशन सुरक्षा ऑडिट और अनुपालन सेवाएं प्रदान करने के लिए एजेंसियों के पैनल में शामिल करने के प्रस्ताव के लिए अनुरोध के लिए।

1. **बोली जमा करने की अंतिम तिथि 18.01.2024 को 15:00 बजे तक बढ़ा दी गई है और इसे 19.01.2024 को 15:30 बजे खोला जाएगा।**

2. **इस शुद्धिपत्र के माध्यम से आरएफपी के संबंधित अनुभागों में संशोधन इसके साथ संलग्न है और इस शुद्धिपत्र को प्रकाशित निविदा दस्तावेज़ के साथ पढ़ा जाएगा (अनुलग्नक - ए)।**

3. **प्रश्नों का उत्तर इसके साथ संलग्न है (अनुलग्नक - बी)।**

Annexure-A (Corrigendum)

TENDER NO. NICSI/Application Security Audit/2023/05

Request for proposal for Empanelment of Agencies for Providing Application Security Audit and Compliance Services

The modification in respective sections of the RFP vide TENDER NO. NICSI/Application Security Audit/2023/05 through this corrigendum is as below and this corrigendum shall be read along with the published tender document:

S. No.	Section	Clause	Reference Page No.	Existing Clause/Section	Modified Clause/Section
1	12. SLA AND PENALTY	Application Security compliance Assessment and Reporting	33	**Applicable Penalty:** 20% of the respective work order	**Applicable Penalty: 10**% of the respective work order

Annexure-B

Query Responses for TENDER NO. NICSI/Application Security Audit/2023/05 "Request for proposal for Empanelment of Agencies for Providing Application Security Audit and Compliance Services"

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
1	Section - 1 - FACTSHEET	5	Pre Bid queries submission last date:	We are keen to participate in this project and look forward to demonstrating our solution approach, experience in similar type of work, sharing our proven global methodologies and profiles of our multi skilled team members for your evaluation. Also, after the addressal of our queries we would require additional time to get internal approvals. Hence, for preparing a comprehensive and best responsive proposal, **we would like to request an extension of the timeline of proposal submission by at least three weeks from the current submission date.**	Please refer to Corrigendum
2	Section - 4 SCOPE OF WORK	9	Issuance of Certificate of 'safe for hosting'	We reuest to please confirm if the empanlled agency will provide an executive summary having Safe for hosting compliance status and the detailed report, which should be considered as the final deliverable. Please note that obtaining a legally recognized certificate is not within the scope of the empanelled agency, as it needs to be obtained from accredited certification providers.	No Change
3	Section - 8.2 FINANCIAL EVALUATION, Point No. b	24	The lowest quoting vendor (L1) in each category will be the bidder with the lowest Gross Total Value (GTV) among all the quoted eligible GTV in the Abridged Financial Bids (Annexure-6: Abridged Financial Bid).	Please clarify if the selection will be on L1 basis as mentioned in the said clause or QCBS as mentioned on Page 60 ANNEXURE-7: DETAILED FINANCIAL BID (B. Penetration Testing and Comprehensive Security Assessment)-- "The Evaluation Committee will select the Agency by giving 70% weightage to the concept and designs (technical evaluation) and 30% weight age on the price bid (financial evaluation)."	**Current empanelment is based on L1 mode.** Annexure-7, Clause vii. in page 60: QCBS is for only for CSA related scope mentioned post empanelment amongst the empaneled vendors.

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
4	Section - 12 SLA AND PENALTY	33	The Auditing agency must submit the Audit/ PT/ Comprehensive Security assessment report and maintain adequate accuracy rate, failing which the penalty as per the following slabs will be applicable. Percentage of Vulnerabilities Reported Applicable Penalty >=95% None >=90% but <95% 2% of the respective work order >=85% but <90% 3% of the respective work order >=80% but <85% 4% of the respective work order <80% but >=60% 8% of the respective work order <60% 20% of the respective work order	Our understanding is that NICSI and empanelled vendor will mutually agree on the framework/formula for calculation of above percentage. Additionally, basis the Clause 9.3 S.No. i. (Page 28) we understand that the overall penalty for the engagement has been effectively capped to 10% of the order value. Please confirm if our understanding aligns with yours or clarify if there are other implications that we should be considering.	Please refer to Corrigendum
5	Section - 12 SLA AND PENALTY	33	If any website/portal/Mobile App/ application security compliance tested by an auditor of an empaneled Auditing agency deployed at NIC/NICSI is defaced or corrupted and is proved to be caused through a vulnerability not highlighted in the audit report, the concerned Auditing agency shall be charged penalty of 5% of respective work order (of the respective slabs) for per reported vulnerability as per the following:	The vulnerabilities on the website/portal/mobile app/application, etc., can occur as a result of various factors, such as configuration changes, upgrades, modifications, or changes in access rights etc. of supporting infrastructure. It is possible that during the vendor's testing phase, the version tested did not contain these vulnerabilities, but they subsequently emerged due to the above-mentioned changes/upgrades. Therefore, we request that in such scenarios, the empanelled vendor will not face penalties, and they will be given the opportunity to conduct an analysis for such instances.	No Change
6	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-	52	Bidder must have an average annual turnover of INR 10 Crore or equivalent amount in any other foreign currency during last three (3) financial years i.e., 2020-21, 2021-22, 2022-	We understand that, NICSI is willing to empanel firms having sound financial and rich experience of handling similiar type of engagemnets. Therefore, may we request to increase the turnover criteria to Rs. 50 Cr.	No Change

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
	QUALIFICATION) , Point No. 12		23 from application security services only.		
7	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION) , Point No. 13	53	The bidder should have experience of at least 3 years in providing Information Security Audit and consulting services as on the date of bid submission.	We understand that, NICSI is willing to empanel firms having sound financial and rich experience of handling similiar type of engagemnets. Therefore, may we request to ammend the clause as below: The bidder should have experience of at least 5+ years in providing Information Security Audit and consulting services as on the date of bid submission.	No Change
8	ANNEXURE-4: ELIGIBILITY COMPLIANCE SHEET(PRE-QUALIFICATION) , Point No. 14	53	The bidder must have executed a minimum of fifteen (15) major projects in last 3 years related to (i) Application Security Audit (ii)Application Penetration Testing (iii) Database Security in any Government (Central / State / PSUs) departments or private organizations with at least three or more projects executed in Government and at least ten executed in India. Note: Each project value should be more than 3 Lakh	We understand that, NIC is willing to empanel firms having sound financial and rich experience of handling similiar type of engagemnets. Therefore, may we request to ammend the clause as below: Note: Each project value should be more than 15 Lakh	No Change
9	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA, Point No.1	55	Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 10 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	We understand that, NICSI is willing to empanel firms having sound financial and rich experience of handling similiar type of engagemnets. Therefore, may we request to increase the turnover criteria to Rs. 50 Cr. Average annual turnover from application security during 3 FYs. i.e., 2020-21, 2021-22, 2022-23. • For Average annual turnover 50 Crores- 5 Marks • For each additional 2 Crores- 1 Mark	No Change
10	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA, Point No.7	56	No. of Projects executed in last 3 Financial Years i.e., FYs. 2020-21, 2021-22, 2022-23 • For 15 Projects- 5 Marks • For each additional 5 Projects- 2 Marks	We understand the "no of projects" mentioned here means no. of similar projects. Please confirm	Yes

S. No.	Relevant Section / Annexure of RFP	RFP Page No.	Relevant Content from RFP	Vendor's Query / Comment	Response
11	ANNEXURE-5: TECHNICAL EVALUATION CRITERIA, Point No.9	56	The organization should have at least 7 security assessment solutions including vulnerability assessment and application testing automated tools. • For 3 commercial licenses out of 7 security assessment solutions- 3 Marks • For each additional commercial license- 1 Marks	May we request you to please ammend the clause as follows: The organization should have at least 5 security assessment solutions including vulnerability assessment and application testing automated tools. • For 2 commercial licenses out of 5 security assessment solutions- 3 Marks • For each additional commercial license- 1 Marks	No Change
12	Termination	NA	NA	May we request you to please add the following clause: "Empanelled Agency may terminate this agreement, or any particular services, immediately upon written notice to NIC/ NICSI/ User Department if Empanelled Agency reasonably determine that it can no longer provide the services in accordance with applicable law or professional obligations."	No Change

For any information, other modifications and/or corrigendum may kindly visit https://etenders.gov.in/eprocure/app.

Sd/-
(Authorized Signatory)