Tel/ Fax: 0381 – 235 5751
e-mail : it.tripura@gmail.com
website: - http://ittripura.gov.in

TRIPURA STATE COMPUERISATION AGENCY

(A Society of Directorate of Information Technology, Govt. of Tripura)
ITI Road, Indranagar, Agartala – 799 006

Notice Inviting Quotation for selection of Agency for Web-application Security Audit Service

Sealed quotation as per the Financial Quotation format (point - E) are hereby invited by Member Secretary, Tripura State Computerisation Agency, (A society under Directorate of Information Technology, Govt. of Tripura), IT Bhavan, ITI Road, Indranagar, Agartala-6 from the **CERT-In empaneled** agency for Web-application Security Audit Service which should be "Guidelines for Indian Government Websites (GIGW)" compliance. The quotation must be accompanied with documentary proof of bidder's CERT-In empanelment.

The interested agencies may drop the quotation at the office of the undersigned (given above) on or before 11th December 2020 by 3 P.M.

The society reserves the right to reject any or all quotation(s) without assigning any reason.

Member Secretary,
Tripura State Computerisation Agency.

A. Scope of work

The main objective of this project is to appoint third-party auditing agency from the CERT-In empaneled Information Security Auditing Organizations those will assist Govt. of Tripura to review the security implementation across the various Govt. Departments and other Clients in the State Department's CMS based Websites/ Portals/ Applications. The agency will also assist the Govt. Departments and other Clients, in identification of the vulnerabilities during assessment & provide recommendations to cope with those vulnerabilities. This will be the stepping stone towards Cyber Safe Tripura.

The Indicative Security Checks to be performed by the selected agency are mentioned below:

1. Application Code Testing

i. Manual testing of code

ii. Automated testing of code

iii. Functional/controls audit

2. Web Application Security Assessment (WASA)

Assessment of all web applications. The web application security assessment should cover the following phases and steps

i. Threat Modelling

ii. Black Box Testing

iii. Grey Box Testing

iv. Reporting

3. Mobile Application Security Assessment (MASA)

Security assessment of all mobile application across all platforms (Android, iOS etc.).

4. Remediation Support

The empaneled agency will give remediation recommendations only to close the vulnerabilities and observations identified. Security issues that pose an imminent threat to the system are to be reported immediately.

5. Issuing of Audit Certificate (Secured for Hosting):

The agency will issue Audit Certificate (Secured for Hosting) after closing of all the vulnerability issues.

Note:

The Bidder is required to perform a detailed security assessment for the assigned entity offering services. The Bidder is expected to prepare the audit checklist based on the responsibilities, risk and the information managed by the entity as well as the information security guidelines and controls as per GIGW.

B. Terms & Conditions

1. The agency either empaneled with Cert-In or any agency that has cleared up-to "Personal Interaction Session (PIS)" but "subject to outcome of background verification" is eligible to participate in this quotation process.
2. If any agency which is under "subject to outcome of background verification" is selected in this quotation process, they will be awarded the work order but payment will be withheld till the agency is formally empaneled by Cert-In.
3. Price should be quoted as per the given format in section-E, failing which quotation will be rejected.
4. Payment shall be released against successful audit completion of each site as per the payment schedule mentioned in section-D of this notice inviting quotation.
5. The bidder must submit CERT-In registration number and contact details of the agency along with financial quotes.

C. Timelines

Sl.	Activities	Timeline
1	Submission of first Security Audit/Assessment Report	10 days from the date of access given to the site in appropriate environment
2	Submission of Re-Audit report based on the vulnerabilities identified from first report.	7 days from the intimation sent about steps taken as per first audit report
3	Submission of Re-Re-Audit report based on the vulnerabilities identified from second report.	7 days from the intimation sent about steps taken as per second audit report

D. Payment Schedule

Sl.	Milestone	Percentage
1	Submission of first Security Audit/Assessment Report	30%
2	Submission of Re-Audit report based on the vulnerabilities identified from first report.	30%
3	Submission of Re-Re-Audit report based on the vulnerabilities identified from second report.	40%

E. Financial Quotation

Sl.	Item Description	Unit	Job	Basic Unit rate (inclusive of all taxes)
1	Web application security audit - 1 static application	1	Job	
2	Web application security audit – 1 dynamic app (1-25 fields)	1	Job	
3	Web application security audit – 1 dynamic app (26-100 fields)	1	Job	
4	Web application security audit – 1 dynamic app (101-200 fields)	1	Job	
5	Web application security audit – 1 dynamic app (>200 fields)	1	Job	
6	Dynamic Web application security audit for 1 year (any number of fields). Audit to be conducted once in 3 months	1	Job	
7	Mobile App security audit for 1 year (any number of fields for both Android and IOS). Audit to be conducted once in 3 months	1	Job	