भारत सरकार
GOVERNMENT OF INDIA
सीमा सुल्क आयुक्त का कार्यालय (बंदरगाह)
OFFICE OF THE COMMISSIONER OF CUSTOMS (PORT)
सीमा सुल्क सदन, १५/१, स्ट्रैन्ड रोड, कोलकाता - ७००००१
CUSTOM HOUSE, 15/1, STRAND ROAD, KOLKATA 700001
PHONE: 91-33-22436493 FAX: 91-33-22435998

FNO S40-01/2016 EDI   Dated:07.08.2019

NOTICE INVITING TENDER FROM CERT-IN EMPANELED AGENCIES THROUGH E-PROCUREMENT FOR CONDUCTING THE SECURITY AUDIT OF KOLKATA CUSTOMS WEBSITE.

Online e-tenders through e-procurement (www. eprocure.gov.in) under two bid system (Technical and Financial Bid) are invited **Only** from empaneled organization of CERT-In for conducting the Security Audit of Kolkata Customs Website (http://kolkatacustoms.gov.in/).

The technical and financial terms and conditions of the AMC shall be as follows:

A. Technical Terms and Conditions

The website is to be hosted at NIC server after Security audit, so the security audit certificate should be in compliance with the NIC standards. The bidders may well acquaint themselves with NIC standards before applying for tender.

Only those who fulfill the following minimum criteria may submit their bids:

i) The bidder must be an empaneled auditor of CERT-In, having valid empanelment certificate. Copy of authorization with valid CERT-in empanelment to be furnished.

ii) Documentary evidence of firm's GST Registration/ PAN/TIN shall be furnished. Bids not satisfying the above eligibility criteria / not accompanied by the requisite documentary proofs shall be rejected.

iii) The bidder must submit an undertaking as in **Annexure-A** that it has not been blacklisted by any government department/autonomous bodies and/or any institutions.

iv) The bidder must submit the details as in **Annexure-B** duly filled by the authorized signatory of the firm & this is to be submitted with Technical Bid.

v) The bidder must have successfully completed minimum three (3) Security Audits in CPSUs / Govt. Organizations during last three years. It is desirable that the Firm/Agency profile should include previous experience of contracts with Government Department. Copy of work order and completion certificate shall be attached.

vi) It should be willing to take up the contract on the terms and conditions as mentioned in the tender document.

vii) The address of the office/workshop with Telephone Nos. /Fax nos. /E. mail address in Kolkata (if any) should be furnished.

viii) A copy of this Tender Notice signed and sequentially numbered by the bidder on all pages, has to be returned with the bid as the same will be treated as the contract between the bidder and the department on successful bidding.

ix) The documents and information, as mentioned above, should be submitted with **Technical Bid**."

x) **Earnest Money: -**

a) All Bids must be accompanied by Earnest Money for an amount of Rs.5,000 (Rupees Five thousand only) in the form of Demand Draft issued by any Scheduled / nationalized bank of India drawn in favor of Commissioner of Customs, Port payable at Kolkata and valid for a period of **forty-five** days beyond the final bid validity period. The Demand Draft may be sent in a sealed envelope to "**Deputy Commissioner of Customs, EDI Port, 15/1 Strand Road, Custom House, Kolkata 700001**. "

b) In case the Bidder claims for waiver of EMD, the bidder shall provide documentary proof of being registered with the Central Purchase Organization, National Small Industries Corporation (NSIC) or the concerned Ministry or Department. The registration must remain valid till the Bid Validity period.

c) Bids without Earnest Money or documentary evidence for waiver of the same as indicated above shall be summarily rejected as non-responsive.

d) Unsuccessful bidder's EMD will be returned within 30 days from the date of placement of order to the successful bidder.

e) The successful bidder's EMD will be released along with the final payment to it on completion of the work. In terms of this clause and if required by the Kolkata Customs, successful bidder will have to extend validity of their bid security.

f) No interest is payable on the EMD.

xi) The Financial bids of firms, who fail to fulfill any of the above conditions, will not be considered.

B. Financial Terms and Conditions

i) The quoted rates on comprehensive basis should contain only the rates.

ii) The amount of contract should include GST and all other taxes, if applicable.

iii) Only the firms meeting the above financial terms & conditions should submit their Bid. The firm which fails to fulfill any of the above conditions will be disqualified.

Both the bids (Technical and Financial) should be super-scribed "**Notice Inviting Tender from CERT-IN empaneled agencies through e-procurement for conducting the security audit of Kolkata Customs Website**." should be addressed to the Deputy Commissioner of Customs, EDI (Port), Custom House, 15/1, Strand Road, Kolkata – 700 001, through **E-Procurement portal** *ONLY* **(No hard copy to be sent) latest by** 30 August 2019

C. Scope of the Security Audit of Kolkata Customs Website.

The Kolkata Customs Website is hosted at National Informatics Centre (NIC) Server as mentioned below:

Organization	Indicative no. of Dynamic Pages (approx.)	Indicative no. of Static Pages (approx.)	Total No. of Input Fields (approx.)	URL	Onsite/ Offsite Audit/ via VPN
Kolkata Customs	161	1	189	http://kolkatacustoms.gov.in/	VPN

To ensure that the Kolkata Customs Website is free from the vulnerabilities, the audit exercise will need to undertake the following activities:

i) **A1- Injection**- Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

ii) **A2.- Broken Authentication and Session Management**- Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities

iii) **A3-Cross-Site Scripting (XSS)**- XSS flaws occur whenever an application takes untrusted data and sends. it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

iv) **A4- Insecure Direct Object References** - A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data

v) **A5-Security**- Misconfiguration Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Scanned by CamScanner

vi) **AS-Sensitive Data Exposure**- Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

vii) **A7-Missing Function Level Access Control**- Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

viii) **AS-Cross-Site Request Forgery (CSRF)-** A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

ix) **A9-Using Components with Known Vulnerabilities**- Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

x) **A10-Unvalidated Redirects and Forwards**- Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

xi) Identify the security vulnerabilities, which may be discovered during the security audit including Cross-site Scripting, Broken Links/ Weak Session Management, Buffer Overflows, Forceful browsing, Form/hidden field manipulation, Command Injection, Insecure use of cryptography, Cookie posting, SQL injection, Server miss-configuration, well known platform vulnerabilities, errors triggering sensitive information, leak etc.

xii) Password Policy, Log Review, incident response and forensic auditing, Integrity Checks, Virus Detection, Identification and prioritization of various risks to the Kolkata Customs Website.

xiii) Any other issues, if any.

D. Deliverables and Audit Reports

The selected auditor will be required to submit the following documents in printed format (2 copies each) after the security audit:

i) A detailed report with security status and discovered vulnerabilities weakness and mis-configurations with associated risk levels and recommended actions for risk mitigations.

ii) Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by relevant department of Kolkata Customs, Port .

iii) The auditor will submit the final audit report after the remedies/recommendations are implemented and confirmed with retest.

iv) The final security audit certificate for the Kolkata Customs Website (http://kolkatacustoms.gov.in/)should be in compliance with the NIC standards.

v) All deliverables shall be in English language and in A4 size format.

vi) The vendor will be required to submit the deliverables as per terms and conditions of this document.

vii) **Work Period:** The completion of the work shall not take more than **35 days** from the date of issue of Work Order. Period which covers from commencement of initial audit of identified security vulnerabilities along with remedial solutions/recommendations, fixing those vulnerabilities by concerned department of Kolkata Customs to the issuance of final security audit certificate by the auditing firm.

E. Confidentiality Clause:

The Contractor agrees to hold in confidence any confidential information received by the Contractor, as part of the connectivity process or otherwise, and the Contractor shall maintain strictest of confidence in respect of such confidential information. Any breach of this clause may compel the department to take appropriate legal and penal action against the contractor.

F. Other conditions: -

i. The Contractor shall indemnify the Government from and against any loss, damage, from no fault on Kolkata Customs and shall ensure that Government's interest is protected and safeguard at any cost.

ii. The contractor shall at once inform Kolkata Customs in the event of any of his license being cancelled or he is deregistered or blacklisted or any action taken against him by any authority whatsoever.

iii. The contract can be terminated at any time if the services are not found satisfactory or found deficient in service.

iv. The agency shall have to follow the instructions of officers authorized by the competent authority for this purpose of inspection / supervision of the work any time.

v. The competent authority of Kolkata Customs reserves the right to recover from the agency in any manner possible excess payment made / recoverable / any loss to the Department for the ignorance and negligence of the Contractor which may come to the notice during audit or any other time.

vi. The agency shall not be allowed an escalation / change in the cost during the period of the contract due to inflation of any sort of change of any policy by government, change of by laws or due to any other reason.

vii. All other specifications, requirements and conditions laid down in the Notice Inviting Tender shall mutatis mutandis form part of conditions of the Terms and Conditions.

G. Payment Mode:

i) The payment will be made only after submitting the Security Audit Certificate and Security Assessment Report on completion of Security Audit of the website and submission of bills in triplicate thereof.

ii) No advance payment shall be made.

iii) No claim on account of any price variation / escalation shall be entertained.

iv) Payment will be released after deduction of TDS and other statutory dues as applicable.

v) No claim for interest in case of delayed payment will be entertained.

vi) All payments under shall be made to the account of the Agency.

09/08/2019

(Vivekanand Maurya)
Deputy Commissioner of Customs, EDI Port
Custom House, Kolkata

Scanned by CamScanner

ANNEXURE- A

DECALRATION REGARDING ACCEPTANCE OF TERMS AND CONDITIONS CONTAINED IN THE TENDER DOCUMENT (To be submitted along with the Technical Bid)

To,

The Commissioner of Customs, Port,
15/1, Strand Road,
Custom House, Kolkata – 700001. Date:

Sir,

I have carefully gone through the Terms and Conditions contained in the Tender Notice dated..............regarding conducting the security audit of Kolkata Customs Website under the jurisdiction of the Commissioner of Customs (Port), Kolkata.

I declare that all the Terms and Conditions of this Tender Notice are acceptable to my Company. My Company does not have any terms and conditions of its own in respect of quotation being submitted for the Security Audit. I further, certify that I am an authorized signatory of my Company and am, therefore, competent to make this declaration.

Yours faithfully,

Signature of authorized signatory with date:
Name:
Designation:
Name of firm:
Address:
Office seal:

Annexure-B

(To be filled by the authorized signatory of the firm & this is to be submitted with Technical Bid)

1.	Name of the Organization/Firm	
2	Name(s) of the Proprietors/Partners/director	
3	Registered Address, Telephone (Landline/Mobile) & Fax No./Email no.	
4	Other Address of any branches with their telephone No. and Faxes/Email no.	
5	Address and Contact Number of the Workshop	
6	Whether firm is registered under Company Act	
7	Whether firm is registered under the Central Goods and Services Tax Act	
8	GST Registration Number. Copy of the same to be attached	
9	Permanent Account Number of the firm. Copy of Pan Card to be attached .	
10	Provident Fund Number allotted by Regional Provident Office, if applicable. Copy of the same to be attached.	
11	Total Engineers working under this firm.	
12	Total staff except above Engineers working under this firm.	
13	Name(s) of the Public Sector/Govt Organization to whom similar services have been provided by the firm (Please attach the service Certificate from Govt. Office/Public Sector)	
14	Name of the website, email ID etc. if available.	

Signature of authorized signatory with date:
Name:
Designation:
Name/ Address of firm:
Seal: