

Clarification/details sought by CERT-In empanelled Agencies w.r.t. Limited Tender dated 21.10.2022 invited by TAMP for conducting Security Audit of TAMP website i.e. <https://www.tariffauthority.gov.in> and Clarification/reply of TAMP

A	M/s Centre for Development of Advanced Computing	TAMP's Reply
1	Organization Name (Mandatory field)	TARIFF AUTHORITY FOR MAJOR PORTS
2	Address for Communication (Mandatory field)	4TH FLOOR, BHANDAR BAHAVAN, M.P.ROAD, MAZGAON, MUMBAI
(i)	PINCODE:	400010
(ii)	GSTN details (Mandatory field) & (iii) TAN details (Mandatory field)	27AAAGT0394P1ZN, MUMT09532F
3	Contact Person Details (Mandatory field)	Name : RAJESH S CHANDRAGADE
(i)		
(ii)	Email ID	Email ID: ad-it@tariffauthority.gov.in,
(iii)	Contact No.	Contact No: 022-23792009,
4	Intranet Application or available to public (Mandatory field)	https://tariffauthority.gov.in
5	Web Application Name & URL (Mandatory field)	TARIFF AUTHORITY FOR MAJOR PORTS, https://tariffauthority.gov.in
6	Brief about the website and activities done through the website (Mandatory field)	Para 1 of Annex-I of the tender document may be referred as regard TAMP Website . The activities done on the website includes uploading of Tenders, RTI applications, Orders, Images, banners, videos, Chairman Messsages, Vacancies etc.
7	Will the website/webapplication/webservice available remotely for auditing (Yes/No) <i>(If No, then the auditors will have to travel to client premises and the costs may include the travel and accomodation charges)</i>	Auditing can be done remotely

8	Number of Roles in the application	Presently 3 Users are created for updation of website as given below : i)Administrator - for content uploading and publishing ii)Programmer - for content uploading iii)Intern-IT - for content uploading. Only the Administrator User has control over all website activities.
9	Number of static pages	NIL
10	Number of Dynamic Pages	All pages are dynamic (No. of pages may be taken from TAMP website https://tariffauthority.gov.in)
11	Payment Gateway Integrated with the application (YES / No)	No
12	Number of User Input fields (approximately)	i) One input form i.e Feedback Form having 8 input fields ii) From TAMP Admin Panel there are approximately 100 forms and 400 input fields.
13	Whether the web application contains any Content Management System. If yes, please mention name of the CMS Yes/No	Yes. Web application contains Content Management system, and can be accessed through URL https://tariffauthority.gov.in/Adminpanel
14	Please share sample login credentials , one for each role Yes/No	Login credentials will be shared with the successful Cert-In empanelled Agency after the Award of the contract on their request.
15	Please share SRS or technical document of the website if any is available Yes/No	Yes. Will be shared after the Award of contract to the successful CERT-In empanelled agency
16	Please share previous audit reports if any are done and available Yes/No	
17	Are you maintaining application logs	No. Website is hosted on NIC Cloud Server. On request of successful CERT-In empanelled agency, application logs maintained by NIC will be obtained and provided.
18	Willing to provide server remote connection to collect the log evidences Yes/No In order to get OWASP Top 10 2018 Complainece, this is mandatory. If you	Website is hosted on NIC Cloud Server. As per reply received from NIC in this regard, Remote access control will be provided only with NIC Team, whenever need arises.

B	M/s Beagle Cyber Innovations Private Limited	
19	Can we send detailed technical proposal along with financial bid and bidder de	Yes, as per our Limited tender document No. : F-20019/1/2000-TAMP [205] Vol-XI dated 21.10.2022
20	Is the deployment completely On-Site or remote?	Deployment is remote on NIC Cloud.
21	Is the testing only greybox testing or black box testing or should we be using	Both
C	M/s PRIME INFOSERV LLP	
22	Whether Audit need to process 'onsite' or online	Website is hosted on NIC Cloud Server. Audit needs to be processed online on the Staging server. After resloution of all the bugs, the final code after clearance by NIC to be hosted on the NIC Cloud.
D	M/s Secure Loopholes Ltd.	
23	Web Application Name & Endpoint	TARIFF AUTHORITY FOR MAJOR PORTS, https://tariffauthority.gov.in
24	Accessible Externally/Internally	Externally
25	Operating System of Server	" Windows Server 2012" at Bullet point no. six under Para 5 of Annex-I of Tender Document may be read as "Windows Server 2016" as recently communicated by NIC.
26	Application Server	" IIS version 9" at Bullet Point No seven under Para 5 of Annex-I of Tender Document may be read as " IIS version 10" as recently communicated by NIC.
27	Programming Language	.net Framework 4.5, ASP.Net with C#, Spring.Net Framework,
28	Back-end Database	" SQL Server 2012 " at Bullet point no five under Para 5 of Annex-I of Tender Document may be read as " Microsoft SQL Server 2017" as recently communicated by NIC.
29	No. of user roles	Reply at Sr.No 8 under A above is reiterated.
30	Whether the site contains any content management module(CMS) (If yes then	Reply at Sr.No. 12 under A above is reiterated.

31	Total No of Dynamic Pages	All pages are dynamic (No. of pages may be taken from the website https://tariffauthority.gov.in)
32	Total No. of Static pages	NIL
33	Payment Gateway Integrated with the application (YES / No)	No.
34	Any other details	NIL
E	M/s Avasure Technologies Private Limited	
35	Point no 4b Cert In agency should create staging environment - Query - staging environment is responsibility of TAMP	As per Clause 4 (b) of the Scope of Work of Annex-I, it is clearly mentioned that "Cert-In empanelled agency" should Create Testing/Staging Environment of TAMP website along with test database to be used for Security Audit Purpose. Creating Staging environment is responsibility of selected CERT-In empanelled agency as per the Tender Document.
36	point no 4g engagement of Third party vendor for compliance of all vulnerabilities - <u>Query - as per the best practice after submission of report with recommendation then it is TAMP responsibility to comply the vulnerability with the help of TAMP developer</u>	Clause 4(g) of the Scope of Work in Annex-I, of the tender document explicitly states that,the Selected CERT-In Agency has to engage a separate third party Agency to carry out mitigation/resolution of all the Vulnerabilities/risks raised during Preliminary audit and by NIC. Mitigation of Vulnerabilities /risks must be completed within a span of 15 days of submission of the Preliminary report to TAMP. A report on closure of all the identified vulnerabilities /risks of the website shall be furnished to TAMP. Further, as per clause 4(j) of the Scope of Work, any subsequent findings about risks/vulnerabilities raised by NIC after submission of final security audit report of Cert-In empanelled agency shall also be mitigated by the Cert-In empanelled agency.Thus, as per the scope of work, mitigation of risk/vulnerabilities is the sole responsibility of Cert-In empanelled agency. For this, Cert-In empanelled agency may engage a seperate third party agency.

F	M/s STPI Bengaluru	
37	STPI-B is cert-in empanelled Agency and will conduct the security audit of the application as mentioned in the RFP (i.e. Two Rounds), However the following points will be the scope of customer(TAMP) a) Creation of Testing/Staging environment of TAMP website along with test database. b) Closure of vulnerability. STPI will conduct the audit and share the vulnerability report along with recommendation	Reply at Sr.No 35 and 36 under E above are reiterated.
38	Request you to kindly provide the details of each applications as mentioned below.	
	i) Total No. of Static pages w.r.t each applications(Approx.):	NIL
	ii) Total No. of Dynamic pages w.r.t each applications(Approx.):	All pages are dynamic (No. of pages may be taken from TAMP website https://tariffauthority.gov.in
	iii) Total No .of Input fields w.r.t each applications(Approx.):	a) One input form i.e Feedback Form having 8 input fields b) From TAMP Admin Panel there are approximate 100 forms and 400 input fields.
	iv) Total No. of user roles(Approx.):	Reply at Sr.No 8 under A above is reiterated.
	v) Database, OS & webserver details of the Web Applications:	Reply at Sr.No 25,26,27 & 28 under D above are reiterated.
G	M/s Xiarch Solutions Private Limited	
39	Web Application URL(Testing or Production url)	https://tariffauthority.gov.in
40	Number of Main URL	One
41	Number of Sub URL	No sub URL
42	Describe Application Used	Reply at Sr.No 6 under A above is reiterated.
43	How many Static Pages are there	Reply at Sr.No.9,10 under A above are reiterated.
44	How many dynamic pages are there	
45	Any payment Gateway used in the Application	No.
46	No. of login modules	Single Administrative Login Module
47	Authorization No. of roles & types of privileges for the different roles	Reply at Sr.No 8 under A above is reiterated.
48	No of input forms	Reply at Sr.No 12 under A above is reiterated.
49	No. (Approximate) of input Fields/parameters	
50	Whether the site contains any content management module(CMS) (If yes then which?)	Reply at Sr.No 13 under A above is reiterated.

51	Whether any payment system, crypto, digital signature, gateway is involved?	No.
52	How many other access rights are there apart from admin?	NIL.
53	Is there any web services involved (If yes then provide details)	No.
54	No of lines	No. of lines may be taken from website https://tariffauthority.gov.in)
H	M/s Bureauveritas (india) private Limited	
55	Source Code for the TAMP website is available with the TAMP office - We understand that the Source Code will be provided to us to install in our system for carrying out the risk assessment. Please confirm our understanding.	Yes.The position is confirmed
56	Cert-In empanelled should create testing / staging Environment of TAMP website along with test data base to be used for Security audit purpose - We understand the testing / staging Environment of TAMP will be created at our premises and testing will be carried out based on the source code / data base provided by TAMP. Please confirm	Yes. Reply at Sr.No 35 under E above may also be referred.
57	The CERT-In Empanelled Agency may engage separate Third Party to carry out mitigation / resolution of all the Vulnerabilities/risks raised during Preliminary Audit and by NIC in their report - Is it mandatory to engage Third Party to carryout mitigation/ resolution of all the Vulnerabilities /risks raised during Preliminary Audit and by NIC? If yes then the selection of TP will be carried out by Cert-In empanelled agency or by TAMP. Please clarify. Alternatively We request that we ourselves issue the mitigation / resolution of all theVulnerabilities /risks raised during Preliminary Audit and by NIC. Please confirm.	a) As per clause 4(g) read with 4(j) of the scope of work, Cert-In empanelled agency may engage a separate third party to carry out mitigation /resolution of vulnerabitites raised during Audit . A report on closure of all identified vulnerabilities is to be furnished . Thus, the use of word "may", shows it is not mandatory to engage third party to carry out mitigation of vulnerabilities raised by NIC and Cert-in empanelled agency as long as the entire scope of work is completed. b) As regards, selection of third party, it is to be done by Cert-In emapanelled agency. TAMP has no role in that.

58	On issue of Final clearance Certificate by NIC, CERT-In empanelled agency to provide necessary technical Support for successful hosting of the secured website content from staging server to live TAMP website..... - Our scope is limited to support TAMP while website hosting for any security related. We will not be responsible for any issues rising out of website Hosting on NIC cloud. Please confirm.	Clause 4(k) of the scope of work is explicit and is reiterated.
59	Not with standing that all reasonable and proper precautions may have been taken by the CERT-In empanelled agency, the service provider shall never the less be wholly responsible for all damage s, if any, to the TAMP - The liability of the service provider is not fixed under this clause. May we request you kindly incorporate the following : Notwithstanding any other provisions, except only in cases of willful misconduct and / or criminal acts, both parties shall not be liable for indirect & consequential loss or damage; and the aggregate liability of the Cert-In-Empaneled Agency/Service Provider in respect of this contract, whether under the Agreement, in tort or otherwise, shall not exceed 100% of the annualized Contract	Clause 13 in Annex-I is a general indemnity . No change is envisaged.
I	M/s Secure Eyes - Infusing Security	
60	Name of the application	TARIFF AUTHORITY FOR MAJOR PORTS, https://tariffauthority.gov.in
61	Please provide brief description of Application and its functionality	Reply at Sr.No 6 under A above is reiterated.
62	Name & Contact details of Developer (Phone No & Email)	Reply at Sr.No 2 and 3(i),(ii),(iii) under A above are reiterated.
63	URL of the target application on test server for audit (Please provide test user credentials to access the application to verify the details.	Reply at sr.no 35 under E above is reiterated
64	Type of Application(Internet or Internet Facing)	Internet Facing

65	Site users (closed user group and/or open to public)	Open to Public
66	How many Login Modules are present in the Application (e.g.for normal user, supervisor, administrator, etc)	Reply at Sr.No 8 under A above is reiterated.
67	Number of Modules and names of the modules in the application(Landing Page, Account summary, etc)	Approx.60-70 Number of Modules & Sub-Modules.
68	How many approximate total number of pages are present in the application?	Reply at Sr.No.10 under A above is reiterated.
69	How many approximate number of dynamic (transactional/taking user input) pages are present in the application?	Reply at Sr.No.9,10 under A above is reiterated.
70	How Many application roles/Privilege levels of users are expected to be in the application?[e.g. end -user with read-only access, supervisors with read and modify access, administrators with create user privileges , help desk engineers with read access etc.]	Reply at Sr.No 8 under A above is reiterated.
71	Development Platform of the Application (For Ex.Java, .Net, PHP etc.)	Reply at Sr.No 25 - 27 under D above are reiterated.
72	What are the external systems with which the application interfaces with?(These include systems like external LDAP authentication servers, Databases, Content Management System, Third Party Payment Gateway , External application APIs etc.)	No external interfaces - except Content Management System.
73	Is there a CMS (Content Management System) present to maintain the application? If Yes, is it in-house built CMS or cutomization of ready to use CMS like joomla, PHP nuke and Drupal etc.?	Web application contains Content Management System (CMS) and can be accessed through URL https://tariffauthority.gov.in/adminpanel .It's a customized CMS in Asp.net.
74	Is there an admin /super-admin module in the application? Is it included in scope of audit.	Website has a CMS to access admin panel. Yes, its part of the scope of audit.
75	What would be the tentative testing environment (Development Staging/ Production Box)	Reply at Sr.No 35 under E above is reiterated.

76	Please provide any additional comments or information that may be relevant	NIL
77	Is there provision for e-commerce and or payment gateway	No
78	No.of phases to test(number of Cycles of audit needed, e,g 1st level audit , 1st level audit + 1 Re-audit or 1st Level audit + 2 Re-Audits)?	Para 4 (c) of Annex-I of the tender document may be referred.
79	Are web services integrated with the application ? If yes , how many	No
80	What are the opearting System details of Developed server(i.e. windows - 2012, Linux, AIX, Solaris	Reply at Sr.No 25 under D above is reiterated.
81	What is the Web/Application Server with version(i.e. IIS5.0, Apache Tomcat, etc)	Reply at Sr.No 26 under D above is reiterated.
82	What is the server side language used [server side scripts](i.e. ASP, Asp.net, JSP, Java, Php)	Reply at Sr.No 27 under D above is reiterated.
83	What are the Back-end Database used? (MS-SQL Server, PostgreSQL, Oracle etc.)	Reply at Sr.No 28 under D above is reiterated.
84	Any target date for the audit to be started?	Immediately after the award of contract.
85	Any target date for the audit to be completed by ?	Time frame for the entire scope of work is 3 months from the date of award of as per clause 6 of the Annex-I of tender document .Completion of audits and mitigation of risks //vulnerabilities can be targetted to be completed by mid to end of Dec 2022.
J	M/s Netrika	
86	No of Dynamic Pages	Reply at Sr.No 10 under A above is reiterated
87	No of Roles	Reply at Sr.No 8 under A above is reiterated.