



सत्यमेव जयते



**महापत्तन प्रशुल्क प्राधिकरण**  
**TARIFF AUTHORITY FOR MAJOR PORTS**  
पत्तन, पोत परिवहन और जलमार्ग मंत्रालय, भारत सरकार  
Ministry of Ports, Shipping and Waterways, Government of India



K-12013/1/2023-IT-Part(1)/7753

I/16146/2023

File No -20019/1/2000TAMP (205)-VOL-XI

Dated: 10.05.2023

To,

Cert-In empanelled agencies as listed in the Tender Document dated 18.04.2023

**Sub:** Clarifications Sought by CERT-In empanelled agencies for conducting the Security Audit of TAMP Website <https://tariffauthority.gov.in> - Reg.

Sir/Madam,

This has reference to TAMP email dated 21.10.2022 under cover of which limited tender No. F-20019/1/2000-TAMP [205] Vol-XI dated 21.10.2022 was invited from CERT-In empanelled agencies to Conduct Security Audit of TAMP website <https://tariffauthority.gov.in>.

2.1 Online Pre-bid meeting was held on 09.05.2023 at 15.00 hrs wherein, clarification sought by CERT-In empanelled agencies was clarified.

2.2 It is to submit that, 7 Nos. CERT-In empanelled agencies have sought clarification/details by email and 12 Nos. CERT-In empanelled agencies who attended the pre-bid meeting on 09.05.2023 have raised queries during the said meeting.

3. Accordingly, a consolidated position of clarification / details sought by total 19 Nos. CERT-In empanelled agencies along with reply of TAMP is furnished herewith as **Annex-I** and **Annex-II** respectively.

4. It is also to mention here that, no further queries will be entertained on the Scope of the Work given in the Tender Document, as most of the queries are already discussed in the pre-bid meeting held on 09.05.2023 and clarified in the **Annex-I & Annex-II** attached herewith.

5. This issues with approval of the Competent Authority.

Yours faithfully,

*Anuradha*

Anuradha Sharma  
(Director)

Enclosure: As stated above.

चतुर्थ तल, भण्डार भवन, मुजावर पाखाडी रोड, माझगांव, मुंबई - 400 010.

4th Floor, Bhandar Bhavan, Muzawar Pakhadi Road, Mazgaon, Mumbai - 400 010.

Tel. : 2379 2000, 2379 2008 Fax : 022-2375 7879, E-mail : [tariff@tariffauthority.gov.in](mailto:tariff@tariffauthority.gov.in), Web : <http://www.tariffauthority.gov.in>

**Queries raised by CERT-In empanelled Agencies w.r.t. Limited Tender dated 18.04.2023 invited by TAMP for conducting Security Audit & mitigation of Vulnerabilities of TAMP website i.e. <https://www.tariffauthority.gov.in> and Clarification/reply of TAMP**

**Queries raised by CERT-In empanelled Agencies**

**Reply/Clarification of TAMP**

A	M/s Dr CBS Cyber Security Services LLP	
1	As per CERT-In guidelines auditors can find the vulnerabilities, mitigation or closure job completed by your developer. Kindly clarify the same	Reference is drawn to para 4(g) of the Tender Document No. : F-20019/1/2000-TAMP [205] Vol-XI dated 18.04.2023 which clearly states as follows: "g. The Cert In empanelled Agency may engage a separate third party to carry out mitigation/resolution of all the Vulnerabilities/risks raised during Preliminary audit and by NIC in their report. 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."
B	M/s Cyber Security Services Team (CDAC Hyderabad)	
2	Organization Name	TARIFF AUTHORITY FOR MAJOR PORTS, <a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a>
3	Address for Communication	4th Floor, Bhandar Bhavan, M.P.Road, Mazgaon, Mumbai - 400010
	(i) PINCODE	27AAAGT0394P1ZN
	(ii) GSTN details	MUMMT09532F
	(iii) TAN details	
4	Contact Person Details (Mandatory field)	RAJESH S CHANDRAGADE
	(i) Name	ad-ii@tariffauthority.gov.in, tariff@tariffauthority.gov.in
	(ii) Email Id	022-23792009
	(iii) Contact No	<a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a>
5	Intranet Application or available to public (Mandatory field)	TARIFF AUTHORITY FOR MAJOR PORTS, <a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a>
6	Web Application Name & URL (Mandatory field)	

7	Brief about the website and activities done through the website (Mandatory field)	Para 1 of Annex-1 of the tender document may be referred as regard TAMP Website . The activities done on the website broadly includes uploading of Tenders, RTI reports, Orders, Images, banners, videos, Chairman Message, Vacancies etc.
8	Will the website/webapplication/webservice available remotely for auditing (Yes/No)	No. The testing/auditing is to be done on staging server to be created by the CERT-In developer. Refer Scope of Work , Para 4 of Annex-1 for details.
9	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.
10	Number of static pages	NIL
11	Number of Dynamic Pages	All pages are dynamic (No. of pages may be taken from TAMP website <a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a> )
12	Payment Gateway Integrated with the application (YES / No)	No.
13	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 approximate 100 forms and 400 input fields.
14	Whether the web application contains any Content Management System. If yes, please mention name of the CMS	Yes. Web application contains Content Management system, its customised CMS in Asp.net and can be accessed through URL <a href="https://tariffauthority.gov.in/Adminpanel">https://tariffauthority.gov.in/Adminpanel</a>
15	Please share sample login credentials , one for each role	Login credentials will be shared with the successful Cert-In empanelled Agency after the Award of the contract on their request.
16	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 on their request
17	Please share previous audit reports if any are done and available Yes/No	Yes. Will be shared after the Award of contract to the successful CERT-In empanelled agency on their request
18	Are you maintaining application logs Yes/No	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.

19	Willing to provide server remote connection to collect the log evidences Yes/No	Website is hosted on NIC Cloud Server. As per reply received from NIC, in this regard the Remote access control will be provided only with NIC Team, whenever need arise.
<b>C</b>		
<b>M/s Allied Boston</b>		
Vulnerabilities Reported by the auditor will be removed /patched /fixed by the client team. Auditing team will not remove/patch/fix any vulnerability		
20		The Scope of work includes mitigation/resolution of vulnerabilities/ risk raised during audit by CERT-In empanelled vendor and Vulnerabilities/risk raised by NIC in their report. Refer para 4 of Scope of Work. Further, the reference is drawn to Clause 9 of para 4 of Scope of Work of the Tender document which clearly states as follows : "9. The Cert In empanelled Agency may engage a separate third party to carry out mitigation/resolution of all the Vulnerabilities/risks raised during Preliminary audit and by NIC in their report. 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."
21	The security audit will be conducted remotely	Reply at Sr. No 8 under B above is reiterated.
22	Web Application Name & URL (if possible dummy username/password) Operating System Details (i.e. Windows-2012, Linux, AIX, Solaris, etc.)	Reply at Sr. No 6 under B above is reiterated. Para 5 of Annex-1 of the tender document gives the Technical details which may be referred.
23		
24	Application Server with Version (i.e. IIS 5.0, Apache, Tomcat, etc.)	
25	Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.)	
26	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	Reply at Sr. No 9 under B above is reiterated.
27	Authorization No. of roles & types of privileges for the different roles	Reply at Sr. No 14 under B above is reiterated
28	Whether the site contains any content management module(CMS) (If yes then which?)	Reply at Sr. No 11 under B above is reiterated.
29	Total No of Dynamic Pages	Reply at Sr. No 13 under B above is reiterated.
30	Total No. (Approximate) of Form Fields are there in the Data Entry pages for Input	One login module for admin panel
31	No. of login modules	NA
32	Mobile application to be audited ? If Yes, please provide type of app (eg., - Native apps - Hybrid apps for all platforms together with Xamarin, React Native, Ionic, Angular Mobile Sencha Touch etc. - Web apps as responsive versions of website to work on any mobile device.	
33	Type of Audit (onsite/Remotely through VPN)	Reply at Sr. No 8 under B above is retained.
<b>D</b>		
<b>M/s Codec Networks</b>		
34	For Mitigation - Do the vendor has to come to onsite location.	No.

<b>E</b>	<b>M/s Event Techsol Pvt Ltd</b>	
35	Do you have a 6 Web APP RIGHT? Kindly provide the size of that application i.e.(Small ,Medium and Large Apps)	It's a .net core version 6. size of application is in between small and medium.
36	Do you want to perform Black Box testing or Gray Box Testing	White Box Testing.
37	Do you want to conduct this activity/remotely or onsite	Reply at Sr.No 8 under B above is reiterated.
<b>F</b>	<b>M/s ISOAEH</b> Sir , We have an inquiry that we have already couriered the tender documents with price quotation to your mumbai office on 18th April 2023 via courier . Please let us know whether you have got it or not or what we have to do in this regard. It will be very kind of you .	Tender received from bidders by courier/ post are directly put in the sealed tender box kept in TAMP office and are opened only on the stipulated date and time mentioned in the tender document. So, we cannot confirm the receipt of your courier at this juncture.
<b>G</b>	<b>M/s Security Brigade</b> Kindly share the Tender Document along with Scope of work details. Also, please share the detailed document for Website mentioning No of user, Modules, Type of audit etc.	Tender document including Scope of Work is already shared to email addresses of the CERT-In empanelled agencies listed in the CERT-In website. The said tender document is also published on the website of TAMP <a href="http://www.tariffauthority.gov.in">www.tariffauthority.gov.in</a> .

**Annex-II**

**Queries raised by CERT-In empanelled Agencies during Pre-Bid meeting dated 09.05.2023 w.r.t. Limited Tender dated 18.04.2023 invited by TAMP for conducting Security Audit & mitigation of Vulnerabilities of TAMP website i.e. <https://www.tariffauthority.gov.in> and Clarification/reply of TAMP**

Sr. No	Queries raised by CERT-In empanelled Agencies	Reply/Clarification of TAMP
A	<b>M/s BDO India LLP - Mr. Ashish Upadhyay and DR CBS CYBER SECURITY SERVICE - Dr. Swati Vashist</b>	
1	a. As per Scope of Work do the CERT-In empanelled agency have to find Vulnerabilities and engage third party to close the Vulnerabilities?	Para 4 Scope of Work attached as Annex I to the tender document may be referred which is explicit. Para 4 'g' of the Scope of Work (SoW) explicitly states that - The Cert In empanelled Agency may engage a separate third party to carry out mitigation/resolution of all the Vulnerabilities/risks raised during Preliminary audit and by NIC in their report. 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."
B	<b>M/s BDO India LLP - Mr. Ashish Upadhyay.</b>	
2	It is difficult to give commercial quote for third party to be engaged to close the Vulnerabilities.	That is for the CERT-In empanelled agency to take a call. Scope of Work is explicit.
C	<b>Mr. Rishi</b>	
3	Whether Mitigation to be done by remotely or we have to come onsite.	Mitigation can be done remotely. It is not required to come onsite. As per clause 4 'b' of the SoW "Cert-In empanelled agency should Create Testing/Staging Environment of TAMP website along with test database to be used for Security Audit Purpose".

<b>D</b>	<b>M/s Security Brigade</b>	All pages are dynamic (No. of pages may be taken from TAMP website <a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a> ) For more details Annex-1 may be referred.
4	Details of Website like how many pages may be provided.	
<b>E</b>	<b>M/s Qseap Infotech Pvt, Mr. Shreyas R.</b>	No.
5	Is there is any sub domain for website	
<b>F</b>	<b>M/s Acquisory Consulting LLP, Mr. Shobhit Sandhiya</b>	Gray box testing.
6	a. It is Black Box Testing or White box testing?  Is there is any login credentials or dummy credentials.	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. No dummy credentials.
	c. Is there any certificate provider from TAMP that as maker and checker from same organization have authority to find Vulnerabilities and close the Vulnerabilities?	As per 4 'j' of the SoW, final security Audit clearance certificate will be issued by NIC. The said clause also states CERT-In empanelled agency has to assist TAMP in obtaining the said final security Audit clearance certificate from NIC.
	d. Will the website/webapplication/webservices available remotely?	As per clause 4 'b' of the SoW "Cert-In empanelled agency should Create Testing/Staging Environment of TAMP website along with test database to be used for Security Audit Purpose".
<b>G</b>	<b>M/s SISA Information Security Private Limited</b>	In this regard Addendum is issued separately.
7	It is requested to extended submission date of Tender Document due to short time for submission of the financial bid by 12.05.2023.	
<b>H</b>	<b>M/s MKS Pvt. Ltd, Ms.Geetu.</b>	As per clause 4 'g' of the SoW "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. TAMP will share the code to the successful Cert- In empanelled agency.
8	a. Is there any time period to find bugs and close the bus?  b. Code level support to fixed bugs is required from TAMP site.	

	c. Is there any extension of time frame will provide if the project is not completed within 3 months? d. This is first time that TAMP is doing Security audit.	As per para 6 of the Tender Document the completion period for entire scope of work will be 3 months from the date of award of work. This is the second time TAMP is doing the Security Audit.
1	<b>M/s. Precise Testing Solution, Ms. Sujata.</b> How much turnover required for this Tender document	All the CERT-In empanelled agencies listed in the tender document at Annex-III are invited by the Limited Tender. No turnover requirement is prescribed in
9		
<b>J</b>	<b>M/s ISOAH Data Securities Private Limited, Mr. Debojit</b>	
10	a. Is there is any criteria for location of vendor. b. How much Extension date of submission for Tender Document ?	All the CERT-In empanelled agencies listed in the tender document at Annex-III are invited by the Limited Tender. There is no restriction of location criteria prescribed in the Tender Document. In this regard Addendum is issued seperately.
11		
<b>K</b>	<b>M/s Security Brigade InfoSec Pvt. Ltd.</b>	
12	a. Kindly share detail of Website like how many pages, module, Input fields, black box and white box testing, normal user, admin user, read only user etc.	All pages are dynamic (No. of pages may be taken from TAMP website <a href="https://tariffauthority.gov.in">https://tariffauthority.gov.in</a> ) For more details Annex-I may be referred, i) One input form i.e Feedback Form having 8 input fields ii) From TAMP Admin Panel there are approximate 100 forms and 400 input fields, White Box Testing is expected, 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. No dummy credentials.
<b>L</b>	<b>M/s. Cybertryz, Mr. Pankaj.</b>	
13	Does the Cert-In agencies have to develop the Staging Server?	As per Clause 4 'b' of the SoW " Cert-In empanelled agency should Create Testing/Staging Environment of TAMP website along with test database to be used for Security Audit Purpose.