No. VP/1899/IT&GTCD/DST Security Audit/2018 Dated 13 December 2022

Corrigendum

Subject: Security Audit & Resolving Critical Vulnerabilities for Website of Department of Science & Technology, Govt. of India (www.dst.gov.in).

In partial supersession of the tender document No. VP/1899/IT&GTCD/DST Security Audit/2018 dated 9 December 2022 on the subject cited above, the scope of work and the last date of submission and opening of tender and Payment terms are being changed as under:

1. **Revised scope of work:**

Para No, of Original Tender Document	Original Scope	Revised Scope
5.5 to 7	The selected agency will have to resolve all vulnerabilities of the DST website from internal and external threats for successful completion of audit of DST website. **1.** The Auditor is expected to carry out a security audit exercise and resolve the critical vulnerabilities, threats and risk identified and reported in the above DST website through Internet Vulnerability Assessment and Penetration Testing. The audit of the DST website should be conducted in conformity with NIC audit guidelines and submit a Security Audit Certificate **7.1. Audit Environment: -** Audit can be done on-site or off-site. The DST website has presently been uploaded NIC Server. **7.2.Roles and Responsibilities: -** The auditor responsibilities need to	1.The Auditor is expected to carry out a security audit exercise, identify and report the critical vulnerabilities, threats and risk identified and reported in the above DST website through Internet Vulnerability Assessment and Penetration Testing**. (Time Frame Seven days)** 2. The audit of the DST website should be conducted in conformity with NIC audit guidelines. The Security Audit Certificate is to be issued after ensuring that the vulnerability pointed out in the initial report have been addressed by the Department (**Time frame: Four days)** **7.1. Audit Environment:-** Audit can be done on-site or off-site. The DST website has presently been uploaded NIC Server. **7.2. Roles and Responsibilities:-** The auditor responsibilities need to

	articulate not just the audit tasks, but also the documentation of their activities, reporting their actions etc. and providing necessary guidance to the developer as and when requested during the audit phase. The auditor also has to resolve the critical vulnerabilities if any and submit the final Security Audit Certificate for the DST website. **7.3. Report:-** Security Audit Report should clearly state that these web-page(s), including the backend database and scripts, if any, are free from any vulnerability and malicious code, which could be exploited to compromise and gain. **7.4.** The final security audit certificate for the DST website (http://dst.gov.in) should be in compliance with NIC standards and submitted to Vigyan Prasar, Delhi Office. **2. DST Website Technical Details:** • Web Server :Apache • Web Application Details: PHP Version 7.1.30 • Framework/CMS Used: Drupal Version 7.69 • Plugins used: jQuery 1.4.4 (collecting information) • Database server: MySQL Version 5.6.44 • Operating system: RHEL	articulate not just the audit tasks, but also the documentation of their activities, reporting their actions etc. and providing necessary guidance to the developer as and when requested during the audit phase. The auditor has to ensure that critical vulnerabilities pointed during audit have been resolved and submit the final Security Audit Certificate for the DST website. **7.3.Audit Report:-** Security Audit Report should clearly state that these web-page(s), including the backend database and scripts, if any, are free from any vulnerability and malicious code, which could be exploited to compromise and gain. **7.4.** The final security audit certificate for the DST website (http://dst.gov.in) should be in compliance with NIC standards and submitted to Vigyan Prasar, Delhi Office. **3. DST Website Technical Details:** • Web Server : Apache • Web Application Details: PHP Version 7.1.30 • Framework/CMS Used: Drupal Version 7.69 • Plugins used: jQuery 1.4.4 (collecting information) • Database server: MySQL Version 5.6.44 • Operating system: RHEL
5 to 5.4	**PAYMENT TERMS** The payment will be made only after submitting the Security Audit Certificate with all the technical support necessary for resolving the security issues and on completion of Security Audit DST website. **5.2.** No advance payment shall be made. **5.3.** No claim on account of any price variation / escalation shall be entertained. **5.4.** Payment will be released after deduction of TDS and other statutory dues as applicable after the receipt of	The payment will be made as under: (i) 40 percent on submission of preliminary report highlighting the vulnerabilities, if any. (ii) 60 percent on submission of Security Audit Certificate

	bill. No claim for interest in case of delayed payment will be entertained by DST.	
B and C of the table on the top of the tender document	**Time and Last date of submission**	**15 December 2022 by 12.00 Noon**
	Opening of Bid	**15 December 2022 at 03.00 PM**

Note

(i) Note: Professional is only to be quoted for Security audit.
(ii) Critical Vulnerabilities will be resolved addressed by Department

(Registrar)