

**DEPARTMENT OF SOIL SURVEY & SOIL CONSERVATION****Directorate HQ**

Vazhuthacaud, Thiruvananthapuram

email: soildirector@gmail.com; Phone: 0471-2778760/1

No: SSSC/1182/2026-PG3

Date: 29-09-2026

QUOTATION DOCUMENT

Sub: Invitation of Quotation for the Cyber Security Audit of three Virtual Machines (VM) and Associated ArcGIS Enterprise Components

The Department of Soil Survey and Soil Conservation, Government of Kerala, invites competitive single-cover quotations from CERT-In Empanelled Agencies for carrying out a comprehensive cyber security audit of the three Virtual Machines (VM) and Associated ArcGIS Enterprise Components to be hosted at the Kerala State Data Centre (KSDC).

Application technical details and specific testing requirements are attached as Annexure-I for reference.

SCHEDULE:

- Last Date & Time of receipt of quotation: 15.10.2026 before 5:00 PM
- Quotation Opening Date & Time: 16.10.2026 at 11:00 AM

TERMS AND CONDITIONS / ELIGIBILITY CRITERIA FOR SUBMISSION OF QUOTATIONS**1. Clause 1 – Eligibility:**

Only organisations/agencies having a valid CERT-In empanelment for providing Information Security Auditing Services on the date of opening of quotations shall be eligible. Documentary proof of valid empanelment shall be submitted along with the quotation. The Department will independently verify the empanelment status from the official CERT-In list.

2. Clause 2 – Submission Procedure:

Single Cover Quotation addressed to the Additional Director, Soil Survey, should be submitted with the subject line "Quotation for VM Security Audit

- SSSC/1182/2026-PG3" physically before the due date and time (15.10.2026 before 5:00 PM). Incomplete, conditional, unsigned quotations, or those received after the deadline will be summarily rejected without further notice.

3. Clause 3 – Compliance with CERT-In Guidelines:

The audit shall be conducted in accordance with the latest applicable CERT-In guidelines, directions and audit requirements, including the CERT-In Comprehensive Cyber Security Audit Policy Guidelines and applicable guidelines for secure application design, development, implementation and operations, as amended from time to time.

4. Clause 4 – Scope of Vulnerability Assessment:

The VMs and ArcGIS Application/WebGIS Workspace shall be comprehensively audited, within the approved scope of work detailed in Annexure-I, to identify known and reasonably discoverable security vulnerabilities using appropriate industry-standard methodologies, tools and manual testing techniques, with the objective of strengthening the overall security posture of the system.

5. Clause 5 – System Access & Cooperation:

The required access to the VMs will be provisioned to the selected auditor in coordination with the KSDC team. The auditor shall cooperate fully, maintain technical evidence supporting reported findings, and provide necessary technical details or logs as requested by the Department.

6. Clause 6 – Support for Remediation and Verification:

The selected security auditor shall provide necessary technical clarification and recommendations to the Department/KSDC technical team for remediation of vulnerabilities identified during the audit. The auditor shall subsequently conduct follow-up/verification testing to confirm the closure of such vulnerabilities.

7. Clause 7 – Audit Report and Certificate:

The final security audit report and certificate shall conform to the applicable CERT-In requirements and KSDC guidelines.

8. Clause 8 – Payment and Safe-to-Host Certificate:

Payment will be processed only after successful completion of the security

audit, remediation/closure of identified vulnerabilities, completion of follow-up/verification testing, and submission of the final 'Safe to Host' certificate and audit report by the CERT-In empanelled auditor, in accordance with the applicable CERT-In and KSDC requirements. No claim for interest or additional charges in case of administrative delays in payment processing will be entertained by the Department.

9. Additional Clause 9 – Confidentiality and Security of Audit Data:

All credentials, logs, source code, configuration details, audit artefacts, reports and other information accessed or generated during the audit shall be treated as confidential and shall be stored, transmitted and handled securely in accordance with applicable CERT-In requirements and the directions of the Department/KSDC. No such information shall be disclosed to any third party without prior written approval of the Department, except where disclosure is required under applicable law or CERT-In requirements. The selected Auditor shall execute a Non-Disclosure Agreement (NDA) with the Department prior to commencing work.

10. Additional Clause 10 – Audit, Remediation and Re-test Timeline:

The audit shall be completed within 15 working days from the date of provision of all required access, information and test environment. The Auditor shall submit the initial audit report within 3 working days of completion of testing. Follow-up verification shall be conducted after remediation of the identified vulnerabilities.

Digitally signed by
Dathan C S
Date: 29-09-2026
15:59:49

Additional Director Soil Survey

Encl: Annexure 1