Providing Cyber Security Audit Services by CERT–In certified firms for Web-based Road Asset Management System (RAMS) Application developed under HP State Road Transformation Project.

1. Introduction

The Government of Himachal Pradesh (GoHP) is implementing Himachal Pradesh State Roads Transformation Project (HPSRTP) with financial assistance from the International Bank for Reconstruction and Development (IBRD). Development and implementation of a Road Asset Management System (RAMS) for the Himachal Pradesh Road Infrastructure Development Corporation Limited (HPRIDCL) as well as the Himachal Pradesh Public Works Department (HPPWD) in one of the mandates of HPSRTP.

As a part of this initiative, HPRIDCL (Client) intends to engage a CERT-in certified Software Security Auditor (Agency) as consultant to audit the Road Asset Management System (RAMS) application portal currently being developed for the security vulnerabilities.

2. Objective

The Road Asset Management System (RAMS) application is envisaged as a system which will serve all level of HPRIDCL and HPPWD to effectively plan and prioritize capital and maintenance works on the state road network. This application will help to improve the quality of decision making in delivery of services related to management of the road network.

This application is planned to be hosted on a cloud platform approved by Ministry of Electronics and Information Technology; Government of India (Meity). The Client desires that the application be CERT-in certified for all the security vulnerabilities in the production environment. Further, the application is required to be annually assessed for a period of three years ensuring that the software is CERT-in complaint at all-times during the 3-year project period.

3. Requirements & Broad Scope

This security audit shall comprise of the following tasks:

- Task 1: Web Application Security Testing, re-testing to confirm closure of Vulnerability
- Task 2: Mobile Application Security Testing, re-testing to confirm closure of vulnerability
- Task 3: APIs Security Testing, re-testing to confirm closure of vulnerability
- Task 4: Issuance of “Fit for Hosting” certificate.

The security auditing shall cover the following tentative parameters as detailed in the following table.

S. No.	Parameters	Description
1	**Web Application Name & URL**	Will be shared with the successful bidder
2	**RAMS Consultant Contact Details**	Will be shared with the successful bidder
3	**Application will be host on**	Cloud Server
4	**Application Server with Version**	IIS
5	**Front-end Tool [Server side Scripts]**	Asp.net
6	**Back-end Database**	MS-SQL
7	**Operating System Details**	Windows

S. No.	Parameters	Description
8	**Whether the application contains any content management module (CMS)**	No
9	**Authorization No. of roles & types of privileges for the different roles**	3 Roles. Administrators, Data Managers, Regular Users
10	**Total No. (Approximate) of Input Forms**	50
11	**Total No. of input fields**	1534
12	**No. of login modules**	Mobile and Web application
13	**Is there any payment gateway ?**	No
14	**Whether audit to be conducted remotely? Yes or NO**	Yes
15	**Whether application/website was audited earlier. If yes, then mention the year also.**	Yes - 2021
16	**Is application behind any WAF (Web application Firewall)?**	Yes
17	**Number of Web Services, if any**	79
18	**Number of methods in all web services**	1035
19	**Number of Input Fields in methods of web services**	1500
20	**No. of Dynamic Pages**	10
21	**No of Screens**	15 per Mobile app
22	**Type of Mobile application**	Android and IOS

4. Detailed Requirements

4.1.1. *Standard*

The standard to be used for Application Testing is through a hybrid approach with OWASP (Open Web Application Security Project) and NIST frameworks (NIST SP 800-53). The Top Ten Most Critical Application Security Vulnerabilities to be covered as given in the following sections. However, the agency will use the most updated OWASP and NIST SP 800-53 guidelines (at the time of auditing) for the top ten critical security flaws for auditing.

4.2. Testing Process

The test will involve checking the Web/Mobile Portal i.e. Functional Test and Penetration testing. The test will assess the effectiveness and Application security. The software application is to be tested with knowledge of the internal workings of an application for which copy of User Manual of the application involving all the defined roles will be shared.

The security consultant will perform the testing with following activities:

- Develop an understanding of the application.
- Develop understanding how application reacts to various input.
- Develop understanding whether application contains common vulnerabilities.
- Run the Test scripts.
- Communicate the Test Results.

This task is expected be undertaken in phases. The First phase Application Audit would highlight the vulnerabilities in the Application like Cross Site Scripting, vulnerability to SQL Injections, Buffer Overflows, Invalidated Inputs, and insecure storage etc. These would need to be addressed by the

RAMS Software consultant, post which the second or third phase audits would be undertaken after some time gap to ensure that the flaws and vulnerabilities as identified in the first or subsequent phases are patched by the consultant of RAMS completely. The security consultant is expected to provide guidance to the RAMS consultant to close the vulnerabilities.

If Vulnerabilities are observed from the re-audit, the RAMS Consultant will re-patch the application and this cycle will continue till all the vulnerabilities have been mitigated.

4.3. Task 1: Web Application Security Testing, re-testing to confirm closure of Vulnerability

4.3.1. *Standard*

The standard to be used for Web Application Testing is through a hybrid approach with **OWASP** (Open Web Application Security Project) and NIST frameworks (NIST SP 800-53).

The OWASP Top Ten represents a broad consensus about what are the most critical application security flaws. The Top Ten Most Critical Application Security Vulnerabilities to be covered as the following,

- A1 Broken Access Control
- A2 Cryptographic Failures
- A3 Injection
- A4 Insecure Design
- A5 Security Misconfiguration
- A6 Vulnerable and Outdated Components
- A7 Identification and Authentication Failures
- A8 Software and Data Integrity Failures
- A9 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery

NIST SP 800-53: Top Ten most critical security vulnerabilities to be covered as the following,

- AC-2 Insufficient Access Controls
- IA-2 Weak Authentication and Credential Management
- SI-10 Unpatched Vulnerabilities
- AU-2 Lack Audit Logs and Monitoring
- SC-12 Inadequate Encryption
- SC-23 Improper session management
- SC-7 Insufficient Boundary Protection
- SC-5 Service Denial-of-Service (DoS)
- CM-6 Improper Configuration Management

4.3.2. *Threats*

Following threats shall be identified from the application software and communicated in the audit reports to be taken-up by the RAMS Consultant.

- **Spoofing of Identity:** Allows an attacker to pose as another user or allows a rogue server to pose as a valid server.
- **Tampering with Data:** Malicious modification of data.
- **Repudiation:** Associated with users denying having performed an action without other parties having any way to prove otherwise.
- **Information Disclosure:** Exposure of information to individuals who are not supposed to have access to it.
- **Denial of Service:** Deny service to valid users.
- **Elevation of Privilege:** An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.

Additionally, the security should also adhere to NIST SP 800-53 or ISO 27001

5. Task 2: Mobile Application Security Testing, re-testing to confirm closure of vulnerability

Mobile Application Security Audit is intended to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.

The security audit shall primarily focus on the application layer and then consider the underlying mobile platform and carrier inherent risks when undertaking threat modelling and building controls.

In addition to the deployment environment, the broader server-side infrastructure with which the mobile apps communicate with should also be covered including integration between the mobile application, remote authentication services, and cloud platform-specific features.

5.1. Standard

The standard to be used for Mobile Application Testing is through a hybrid approach with OWASP (Open Web Application Security Project) and NIST frameworks (NIST SP 800-53).

The OWASP Top Ten represents a broad consensus about what are the most critical application security flaws. The Top Ten Most Critical Mobile Application Security Vulnerabilities to be covered as the following,

- M1 Insecure Data Storage
- M2 Weak Server-Side Controls
- M3 Insufficient Transport Layer Protection
- M4 Client-Side Injection
- M5 Poor Authorization and Authentication
- M6 Improper Session Handling

- M7 Security Decisions Via Untrusted Inputs
- M8 Side Channel Data Leakage
- M9 Broken Cryptography
- M10 Sensitive Information Disclosure

NIST SP 800-53: Top Ten most critical security vulnerabilities to be covered as the following,

- SC-28 Insecure Data Storage
- IA-2 Week Authentication and Authorization
- SC-12 Unsecured communication
- SC-23 Improper Session Handling
- SI-10 Code Injection Vulnerabilities
- CM-6 Code signing and distribution through trusted app stores
- SC-13 Insufficient cryptographic controls
- SC-7 Insecure API usage
- AC-6 Excessive Permissions
- CM-6 Improper Configuration

5.2. Threats

Following threats shall be identified from the mobile application software and communicated in the audit report for further compliance by the RAMS Consultant.

- Unsafe sensitive data storage
- Spyware, Surveillance, Financial malware, UI impersonation
- Network spoofing attacks
- Attacks on backend systems, loss of data via cloud storage: Insecure implementation of backend APIs or services, and not keeping the back-end platform hardened/patched will allow bad guys to directly attack/compromise the back-ends.
- Denial of Service: Deny service to valid users.

6. Task 3: APIs Security Testing, re-testing to confirm closure of vulnerability

The key objective of this Web Service and API Testing was to identify whether any vulnerabilities exist in the Web Service and to exploit those that can be seen and compromised by malicious users. The objective of this testing was to ensure the security of the network and web server from external threats through the web service.

6.1. Standard

The standard to be used for Mobile Application Testing is through a hybrid approach with OWASP

(Open Web Application Security Project) and NIST frameworks (NIST SP 800-53).

The OWASP standard represents a broad consensus about what are the most critical web service security flaws. The following summarizes the OWASP Topmost Critical Web Service Security Vulnerabilities:

Information Gathering

- TC-IG01 WSDL Retrieving
- TC-IG02 Error Message Information leakage

Fuzzing

- TC-FZ01 Numerical Values
- TC-FZ02 Base64 Encoded values
- TC-FZ03 Character Strings
- TC-FZ04 General Values
- TC-FZ05 Session Tokens
- TC-FZ06 Format String Parameters
- TC-FZ07 File Names

Injection

- TC-IN01 SQL Injection
- TC-IN02 Command Injection
- TC-IN03 LDAP Injection
- TC-IN04 XPATH Injection
- TC-IN05 Code Injection
- TC-IN06 XML Special Characters
- TC-IN07 XML CDATA Sections

Confidentiality and Integrity

- TC-CI01 Cipher Choice
- TC-CI02 Encryption Coverage
- TC-CI03 Replay Attacks
- TC-CI04 Invalid XML
- TC-CI05 XML Canonicalization

Authentication and Authorization

- TC-AA01 Brute Force and Dictionary Attack
- TC-AA02 Forged Credentials
- TC-AA03 Missing Credentials
- TC-AA04 Authentication Exchange Tampering
- TC-AA05 Man-in-the-Middle Attacks

- TC-AA06 Factors of Authentication
- TC-AA07 Authentication Session Manipulation
- TC-AA08 Storage of Authentication Credentials
- TC-AA09 Confidentiality of Authentication Exchange
- TC-AA10 Certificate verification
- TC-AA11 Token Forgery
- TC-AA12 Hijacking Attacks
- TC-AA13 Temporary Files

Availability

- TC-AV01 Parameter Tampering
- TC-AV02 Coercive Parsing
- TC-AV03 Recursive SOAP
- TC-AV04 Overly Large SOAP
- TC-AV05 Schema Poisoning
- TC-AV06 Authentication Flooding

NIST SP 800-53: Top Ten most critical security vulnerabilities to be covered as the following,

- AC-3 Broken Object-Level Authorization
- IA-2 Broken Authentication
- SC-28 Excessive Data Exposure
- SC-5 Lack Resources and Rate Limiting
- SI-10 Injection Attacks
- CM-6 Security Misconfiguration
- CM-8 Improper Asset Management
- SI-11 Improper Error Handling
- AU-2 Insufficient Logging and Monitoring
- SC-12 Insecure Communication

7. Task 4: Issuance of “Fit for Hosting” certificate

Fit for Hosting certificate should be issued by the consultant once all the vulnerabilities have been closed.

8. Duration

The total duration of the consultancy services will be 3 years during which the agency will be required to conduct the software security audit annually following the time-line as given below.

9. Deliverable and Schedule of Payment

The software security audit will be undertaken annually, during the project period of 3 years. The first audit will be undertaken on the RAMS Consultant platform before hosting on the Meity empaneled cloud platform. The subsequent 2 audits will be undertaken on the cloud platform after migration. After each successful audit, the agency will issue Compliance Certificate recognized by the Meity valid for one year.

Each time the security audit is expected to be undertaken in three phases; each phase of audit will include detailed report for each task separately. The Security Audit Report based upon testing (as per the standard procedure) will describe about identified vulnerabilities and flaws in detail as per guidelines of the Meity. The report will have details of the methodology and tools used in the testing, summary of the vulnerabilities found, detail findings, proof of concept with screenshots and recommendations.

Based on the report, the consultant of the RAMS application will undertake measures to rectify their codes to address the vulnerabilities and communicate with the consultant for subsequent phase audits. A maximum of 8 - weeks (Work days) are allowed for compliance by RAMS Consultant in 1st phase, 5 weeks each in 2nd phase and 3rd phase.

Hosting Clearance certificate will be issued by the consultant only after verifying that all vulnerabilities have been closed as brought out in the audit reports.

The **Security consultant** will be required to submit the following documents after completion of the security audit.

i. A detailed summary report will be submitted detailing the discovered vulnerabilities, the impact of vulnerability with associated risk levels or severity rating, and recommendations for risk mitigations. The detailed report will also give the steps/methods used to establish vulnerability along with the screenshots.

ii. For a given vulnerability, all possible links affected in the application will be specified.

iii. For re-audit reports the previous level summary report needs to be updated, giving the audit level and the updated status of the vulnerability (Open/Closed). In the event a new vulnerability is determined at a re-audit level, a new summary table for that level will be made in the detailed report the consultant will specify the reason for finding the vulnerability at a re-audit stage.

iv. Hosting of clearance certificate should be issued by the consultant once all the vulnerabilities have been closed.

The **RAMS consultant** should submit the following details after completion of the patching.

i. Once the Audit report is submitted to RAMS software consultant, they should address all the vulnerabilities identified in the audit withing the agreed timeline, prioritizing critical and high-severity issues.

ii. Collaborate with the security consultant to clarify findings, seek guidance on remediation strategies, and ensure fixes align with security best practices.

iii. Maintain detailed records of the fixes implemented, including version histories.

Client's responsibilities

i. Act as the single point of contact to coordinate between the Security Consultant and RAMS software consultant.

ii. Ensure all necessary testing environments and resources including hardware/software are available for the audit process.

iii. Monitor timelines and enforce accountability to ensure the RAMS Consultant adheres to deadlines.

iv. Activate an escalation mechanism if the RAMS consultant fails to address vulnerabilities within the stipulated timeframe.

Review committee's Role

i. Review and approve the final follow-up report submitted by the auditor.

ii. Track progress on unresolved vulnerabilities and ensure proper resolution.

iii. Recommended actions if contractual obligations (e.g., timely fixes) are not met by the RAMS software consultant.

Deliverable	**Deliverable Due Date** (from project initiation)	**% Release of payment**	**% Cumulative**
Year 1			
Report on Security Audit (Phase-1) (Task 1, 2 and 3)	Month 1	10	10
Report on Security Audit (Phase-2) (Task 1, 2 and 3)	Month 2.5	5	15
Report on Security Audit (Phase-3) (Task 1, 2 and 3)	Month 3.5	5	20
Audit Certificate for Himachal Pradesh RAMS Application-Year 1 (Task 4)	Month 4.5	20	40
Year 2			
Report on Security Audit (Phase-1) (Task 1, 2 and 3)	Month 13	5	45
Report on Security Audit (Phase-2) (Task 1, 2 and 3)	Month 14.5	5	50
Report on Security Audit (Phase-3) (Task 1, 2 and 3)	Month 15.5	5	55
Audit Certificate for Himachal Pradesh RAMS Application - Year 2 (Task 4)	Month 16.5	15	70
Year 3			
Report on Security Audit (Phase-1) (Task 1, 2 and 3)	Month 25	5	75
Report on Security Audit (Phase-2) (Task 1, 2 and 3)	Month 26.5	5	80
Report on Security Audit (Phase-3) (Task 1, 2 and 3)	Month 27.5	5	85
Audit Certificate for Himachal Pradesh RAMS Application - Year 3 (Task 4)	Month 28.5	15	100

50% Payment will be made to the Consultant on submission of reports and balance 50% on acceptance of the reports/deliverables by the Review Committee.

Review of reports:
A review committee consisting of following officers of the client's Department will review all reports of Consultant and suggest any modifications/changes considered necessary within 30 days of receipt.

1.	Director (Projects), HPRIDCL, Nirman Bhawan, Nigam Vihar, Shimla-171002	Chairman
2.	Executive Director-cum- Superintending Engineer (P&D), HPRIDCL, Nirman Bhawan, Nigam Vihar, Shimla-171002	Member
3.	General Manager (Finance)-cum- Joint Controller, HPRIDCL, Nirman Bhawan, Nigam Vihar, Shimla-171002	Member
3.	Team Leader, Implementation Capacity Gap Consultant	Member

10. Experience and Qualifications of the Consultant firm

The firm shall submit the proofs of minimum eligibility criteria as given below:

(i) The bidder should be empaneled by CERT-IN for IS Audit.

(ii) The Bidder should not have been blacklisted by any State/Central Government Institution or any Public Sector unit. The bidder shall give an undertaking (on their letterhead) that they have not been blacklisted by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was blacklisted by any of the Govt. Authority or PSUs, the name of the company or organization must have been removed from the blacklist as on date of submission of the tender. Undertaking by bidder shall be submitted.

(iii) The bidder should have a minimum average annual turnover of INR 0.30 Crores in the last 3 years i.e. 2021-22, 2022-23, 2023-24. Audited Balance Sheet, Profit & Loss account for the last 3 financial years to be submitted.

(iv) The Bidder should have experience in handling Assignments / Services related to comprehensive security review of Data Centre/Enterprise Network, Active Directory, Application Security, Security review/ IS or IS-IT Audit (including Vulnerability Assessment and Penetration Testing (VAPT)) in India during last five financial years.

(v) Bidder must have carried out Minimum TWO Information Security Audit in Central/State Government/PSUs (or) Banks. Each of the IS Auditshould be with minimum 15 Man-Days duration. Reference Site, Customer Name and Contact information to be provided with whom discussion can be done.

The Consultant is expected to mobilize appropriate number and specialised key personnel along with supporting staff to undertake the envisaged activities. A list of key personnel and the desired qualification, experience, and credentials to be evaluated at the stage of technical proposals is provided below. Consultants are expected to depute other support staff to meet the audit requirements.

Position	Desired Experience
Team Leader/Cyber Security Auditor	• Degree in any relevant field. • He should have suitable auditor qualification and certifications such as CISA / CISSP /ISO 27001 Assessor / ISA or any other formal IT security auditor qualifications etc. • He must have completed minimum 5 IS Audit including one in Central/State Govt / PSUs / Bank. • At least one IS Audit as Lead Auditor.