

ALL INDIA INSTITUTE OF MEDICAL SCIENCES
Bilaspur, Himachal Pradesh

No. AIIMS-BLS/(G)/2023/NIQ/24

Dated: 20 12/2023

NOTICE INVITING QUOTATION
Supply of IT Infrastructure for Security Audit

Sealed quotations are invited from CERT-In empanelled Auditors having GST No. for conducting Cyber Security Audit of AIIMS Bilaspur as per detailed scope of work (Annexure-A). Sealed Quotations in Two envelopes (Technical + Financial) duly super subscribed at the top of the envelope as "**Quotation No. AIIMS-BLS/Stores/2023/NIQ/24 for conducting Cyber Security Audit of AIIMS Bilaspur due date of opening 05-01-2024**" containing both the "Technical Bid" and "Price Bid" (in two separate envelops) may be submitted so as to reach on or before 05-01-2024 up to 11:00 A.M in Procurement Section Ground Floor Admin Block Opposite to Dean Office, AIIMS Bilaspur, Kothipura, Bilaspur, Himachal Pradesh PIN- 174001. Late bids will not be considered. The bids shall be opened in the presence of duly constituted local purchase committee and bidders who may wish to be present on the same day at 11:30 A.M.

For the purpose of technical evaluation, the bidder is required to submit following documents.

Technical Bid:

1. Profile-Name & Full Address of the firm & year of establishment.
2. CERT-In Empanelled authorization certificate.
3. Copy of permanent GST registration certificate.
4. Copies of supply orders secured during 2020-2021, 2021-2022 & 2022-2023 for the similar services.
5. Previous two Income Tax Returns, Profit & Loss Account statement of the firm (FY 2020-2021, 2021-2022 & 2022-2023).
6. Self-declaration that the firm is not debarred by MoHFW or MeitY or CERT-In.
7. The bidder must comply on the Scope of work (Annexure-A).

In case the Technical Committee rejects the firm on technical grounds, the financial bid in respect of that firm will not be considered.

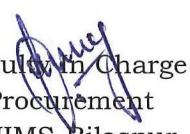
Financial Bid: The rates and total cost must be quoted in both words and figures (over writing not allowed). Selection will be made purely on the basis of lowest price quoted by technically qualified firms. Validity of the quotation should be for a minimum period of 90 days in case discrepancy between unit price & total price, the unit price shall prevail.

Financial Bid submission format for items with quantity required is as under: -

Sr. No.	Description	Unit Price	GST	Total
1	Comprehensive Audit			
2	Limited Audit			
3	Forensic/Incidental Investigation			

Other terms and conditions will be as follows: -

1. Services shall be provided at AIIMS-Bilaspur
2. Delivery Schedule of services shall be as per the Statement of Work. Delayed supplies beyond stipulated time from the date of Supply Order will be subject to LD @0.5% per week or part thereof, on the contract price subject to maximum of 10% of contract price beyond which the supply order will be liable to be cancelled.
3. Bidder is required to quote rate for all the 3 services.
4. Part bidding will not be accepted.
5. No revision in rate (on higher side) will be accepted at any stage.
6. The firm shall not assign or sublet the work/job or any part of it to any other firm.
7. Billing will be in the name of Executive Director, AIIMS-Bilaspur. Payment will be made after the service has been completed and report verified. No advance payment will be made at any stage.
8. Taxes at other government levies will be paid extra as applicable.
9. For any query, please contact on our registered, E-mail stores.aiimsbilaspur@gmail.com


Faculty In Charge
Procurement
AIIMS-Bilaspur
H.P.

SCOPE OF WORK (ANNEXURE-A)

General Terms

The successful bidder shall provide all the mentioned services in Scope of Work. None of the services shall be outsourced to any other third party under any circumstance.

Bidder to use licensed tools for delivering all the services as mentioned in the scope of work.

The Institute shall not bear any cost for the tools and their licenses used for these services.

The Institute shall not provide any tools that may be required by bidder for delivering any of the services as mentioned in the scope of work.

The Institute will not make any additional payment for usage of tools proposed by the bidder.

If from security perspective, the Institute requires that the bidders are required to operate on the Institute systems and not on the bidders' desktops/laptops, the bidders will be required to install tools and operate on the desktop/laptop provided by the Institute to the bidders.

Bidder needs to clearly stipulate activities that will be conducted onsite (at the Institute premises) and those that will be carried out from bidder's premises.

VAPT, Application security audit shall be carried out on Servers/applications hosted either in the Institute's cloud environment or on third party premises, if required, in case some applications are hosted on servers of third-party locations.

Each individual resource (working on the institute project) of the selected bidder has to sign NDA before commencing the activities mentioned in the Scope of Work.

Before deploying any engineer, successful bidder must produce his/her resume along with security certification as evidence to the institute to establish that required eligibility criteria are being met. On successful verification of the engineer's profile, he/she shall be allowed to carry out the required exercise. Any delay due to non-compliance with engineer's eligibility shall be attributed to the successful bidder which, in turn, shall impact the SLA.

Post completion of the activities, successful bidder to deliver the following:

Assessment report of the findings (after filtering the vulnerabilities for false positives) for VAPT, WAPT, Application security assessment, Incident lifecycle review & configuration review. The report should contain:

- i) Identification of auditee
- ii) Date, time and location of the audit
- iii) Standards followed
- iv) Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, application security audit

etc.) with following details:

- a) Tools used and methodology employed.
- b) Positive security aspects identified.
- c) List of vulnerabilities identified.
- d) Description of vulnerability
- e) Risk rating or severity of vulnerability
- f) Category of risks: Very High/ High/ Medium/ Low
- g) Test cases used for assessing the vulnerabilities.
- h) Illustration of the test cases
- i) Proof/ evidence (screenshot) of the vulnerabilities identified.
- v) Analysis of vulnerability and issue of concern
- vi) Recommendation(s) for corrective action as per industry standard and best practices

All the reports submitted should be signed by technically qualified persons and he/she should take ownership of document submitted to the institute

After conducting the assessment and categorizing the risks, bidder should give 30 days (or based on effort required) to close the findings, before they perform the reassessment

Conduct Post VAPT review/audit Compliance after the institute implements the recommendations.

Share final detailed review report & recommendations along with solutions for mitigation of vulnerabilities.

Documents prepared by bidder for the institute will be intellectual property of the institute.

COMPREHENSIVE AUDIT

The engineer who shall carry out the Comprehensive audit must have the minimum qualification as mentioned under:

- I. Must be certified as “CEH (Certified Ethical Hacker)”.
- II. Must have at least 2 years of experience in carrying out VAPT/WAPT activities

Comprehensive audit should cover the entire applications including the following:

- (a) web application (both thick client and thin client);
- (b) mobile apps;
- (c) APIs (including API whitelisting);
- (d) databases;
- (e) hosting infrastructure and obsolescence;
- (f) cloud hosting platform and network infrastructure; and
- (g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

Vulnerability Assessment & Penetration Testing (VAPT)

The engineer who shall carry out the VAPT exercise (either on site or offsite) must have minimum qualification as mentioned below:

- I. Must be certified as “CEH (Certified Ethical Hacker)”.
- II. Must have at least 2 years of experience in carrying out VAPT activities

Any risks associated with the penetration testing to be analyzed and submitted to the institute prior to the activity.

Manual as well as tool-based vulnerability scan shall be performed.

Following testing activities (but not limited) need to be completed in the VAPT testing:

- Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particular; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and

whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);

- Penetration testing
- Security assessments for Interfaces to COTS
- Database security assessments (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication)
- Network and device configuration review
- Application hosting configuration review
- Access and authorization check like Least Privileges access, Segregation of Duties
- User access controls (including privilege access management) and access reconciliation review
- Identity and access management controls review
- Data protection controls review (inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks ICIAD-2021 -0004]");
- Security operations and monitoring review (including maintenance of security logs, correlation and analysis);
- Review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); and
- Review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).

If case required below listed activities may be taken up on need basis:

- i) Network Scanning
- ii) Port Scanning
- iii) Service Identification Scanning
- iv) Vulnerability Scanning

- v) Malware Scanning
- vi) Vulnerability Assessment

Web Application Assessment & Penetration Testing (WAPT)

The engineer who shall carry out the WAPT exercise must have the minimum qualification as mentioned under:

- I. Must be certified as “CEH (Certified Ethical Hacker)”.
- II. Must have at least 2 years of experience in carrying out VAPT activities

Following types of applications shall be tested under WAPT exercise:

- I. Open Source platform (like NodeJS, Flutter, java scripting, etc ...)
- II. Microsoft .NET
- III. Java
- IV. Apache, IIS
- V. Others

Scope of WAPT shall cover Black box testing of all production applications hosted in the Cloud environment.

Grey-box testing to be carried out for all test environment applications hosted in the Cloud environment.

Application Security Audit

The Application Security Audit of website and/or hosted application (Internal & External) should be performed using the tools with considerable manual intervention.

This involves VAPT for interfaces with COTS and SaaS applications, WAPT including Black Box & Grey Box Testing, Source Code Review, Mobile Application Security & Penetration testing, Internal or External Software Risk Assessment and bidder certification.

It also includes any APIs, Adaptors, protocols and data transfer methods exposed and consumed by other systems such as:

- PLC, IOT devices, SCADA, LRC, TAS
- Integration with SAP, Salesforce CRM and other IT applications.

During the Grey Box testing, bidder is expected to test the functionality of the application using more than one role and identify issues that cannot be found using automated scanners.

The number of roles, to be used during grey box testing, will be shared during the testing phase.

Application Security testing shall include testing for common vulnerabilities mentioned in forums such as Open Web Application Security Project (OWASP), but not limited to that.

Grey Box & Black Box Testing - Application Security assessment/testing should be done as per the latest OWASP guidelines including but not limited to the following:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using components with known Vulnerabilities
- Insufficient logging and Monitoring

Any other attacks, which can prove to be vulnerable for web sites and web applications, COTS applications, Interfaces with SaaS solutions.

Find out any other security gaps in the application through other forms of automated and manual testing

Source Code Review

Bidder to review source code of an application to verify proper security controls are present and are working as intended.

The source code review to be carried out must include but must not be limited to

- ‘Format String Missing’,
- ‘Buffer Overflow’,
- ‘Memory Leaks’,
- ‘Security concerns on APIs used’,
- ‘Session management’,
- ‘Authentication’ and authorization

Bidder to identify existing security flaws (if any) and suggest remedial steps.

Mobile Application Review

- Assess the application with respect to user data privacy

- Comprehensive security testing of customized mobile applications prepared on Android, Windows Mobile, Apple iOS, KaiOS, Java application platform, cross platform
- Find out any other security gaps related to mobile applications specific vulnerabilities

Recommendations & Mitigation

Vulnerability Assessment & Penetration testing along with the recommendation(s) and assistance in mitigation to be provided as part of the detailed report that is to be submitted

LIMITED AUDIT

The engineer who shall carry out the Limited audit must have the minimum qualification as mentioned under:

- I. Must be certified as “CEH (Certified Ethical Hacker)”.
- II. Must have at least 2 years of experience in carrying out VAPT activities

The scope of limited audit should include, inter alia, the following:

In all cases

- Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;

Routine limited audit (six months after comprehensive audit)

- Scope of work included in all cases and in addition,
- User access controls (including privilege access management) and access reconciliation review; identity and access management controls review;

Limited audit done earlier (applicable in cases if there is (i) modification in application functionality; or (ii) addition/modification of APIs; or (iii) migration to new infrastructure platform or cloud service; or (iv) change in configuration of application hosting, servers, network components and security devices; or (v) change in access control policy

- Scope of work in Routine limited audit and in addition,
- For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change in configuration of application hosting, servers' network components and security devices or Network

vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorised users and are protected with multifactor authentication); data protection controls review (inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-202 1 -0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solutions, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERI-In may require through directions issued by it in exercise of powers vested in it by law); review of logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

- For audit on change in access control policy; Review of logs and integration with security monitoring solutions

FORENSICS / INCIDENT INVESTIGATION

Forensic would be used for advanced analysis during Incident Management on Cyber Incidents or virus outbreak. In addition, it would be used for finding evidential data, collecting it, preserving it and presenting it in a manner acceptable in a court of law.

The engineer who shall perform the forensic investigation must have the minimum qualification as mentioned under:

- I. Must be certified as "CHFI (Computer Hacking Forensic Investigator)".
- II. Must have at least 3 years of experience in digital forensics

The institute shall approach the successful bidder for below activities under this line item:

1. Obtain understanding of the incident
2. Determine the scope of forensic technology procedures required to be carried out based on the nature of the incident.
3. Carry out any of the following forensic procedures (but not limited to) :
 - a. Determine the cause for compromise of the system
 - b. Hard disk imaging
 - c. Event log analysis
 - d. Internet history analysis
 - e. Seek evidence in cached instances of RAM data
 - f. Firewall logs for analyzing inbound connections to the identified computer
 - g. Gateway log analysis to map inbound traffic with respect to outbound traffic
 - h. Antivirus / System log analysis
 - i. Ransomware incident analysis & data recovery
 - j. HDD normal data analysis
 - k. Discover the source of botnet in case of DoS/DDoS, virus or spam outbreak
 - l. Spam or phishing mail analysis

Prepare a detailed analysis report and present findings to management.

Delivery Schedule (SLA)

- All schedules will be calculated from the date of receipt of request from the institute.

#	Parameter	Timelines
1	Bidder to arrange eligible resources to carry out the request from the institute. Comprehensive/Limited Audit (VAPT, WAPT, Re-validation, Application Security Audits)	Within 7 days from the date of receipt of the request from the institute.
2	Bidder to complete the deliverables as given in SOW	Within 10 days from the date of start of work.
3	Bidder to arrange competent resource for forensic investigation	Within 2 business days from the date of receipt of the request from the institute.

Use of Original Software

The bidder should use only legal / valid software/ licensed tools for delivering any of the services as mentioned in the Scope of work. The institute shall not bear any cost for the tools used for these services. The institute would not be responsible for any use, either direct or indirect, of illegal software by the bidder. The bidder would indemnify the institute against the same.