REQUEST FOR PROPOSAL

For CERT-In Empaneled Security Auditor for Security Audit of Web and Mobile Applications under Vihaan Care and Support Programme

India HIV/AIDS Alliance (Alliance India) is requesting for proposal for services of a qualified CERT-In Empaneled Security Auditor for Security Audit of Web and Mobile Applications under the Vihaan Care and Support Programme. The Alliance India invites you to submit a Proposal to this Request for Proposal (RFP) for the above-referenced subject.

Project Title	Security Audit of Web (Client Management Information System) and Mobile Applications under Vihaan Care and Support Programme
Dates, Duration, Days & Hours	(April 2023 – April -2023)
Location	India HIV/AIDS Alliance, 6 Community Centre, Zamrudpur | Kailash Colony Extension,| New Delhi 110 048

About India HIV/AIDS Alliance

Founded in 1999, India HIV/AIDS Alliance is a not-for-profit operating in partnership with civil society, government and communities to support sustained responses to HIV in India that protect rights and improve health. Complementing the country Programme, we build capacity, provide technical support and advocate to strengthen the delivery of effective, innovative, community-based HIV programmes to vulnerable populations affected by the epidemic. More www.allianceindia.org

About Vihaan Project:

Complementing the Government HIV Programme, the Global Fund-supported Vihaan Care & Support Programme, implemented by India HIV/AIDS Alliance (Alliance India) and its partner, promotes care & support for people living with HIV (PLHIV) to improve the uptake and efficacy of treatment since April 2013 onwards. A core component of India's national HIV strategy, Vihaan offers community-based outreach, follow-up, counselling and referral services for PLHIV to strengthen treatment adherence, increase retention in care, and improve the overall quality of life for PLHIV.

Currently, 310 Care & Support Centers (CSCs) are linked with all functional ART centers across India to provide differentiated care and support services to more than 1.4 million PLHIV by 2021.

The Vihaan consortium is led by Alliance India and National/state-level PLHIV networks and NGOs that partner with district-level PLHIV networks and other organizations to deliver care & support services in communities. Vihaan CSCs are committed to the health and well-being of all PLHIV and their affected families, with a special effort to reach those from underserved populations, including women, children and members of high-risk groups, such as female sex workers (FSWs), men who have sex with men

(MSM), Trans genders, Hijras and People who inject drugs (PWID). Vihaan provides access to a range of quality care & support services using an integrated approach that complements existing HIV prevention and treatment programming. Working in coordination with nearby ART Centers, CSCs serve as safe spaces for PLHIV, offering services that include counselling, outreach and follow-up support, health referrals, and linkages to social welfare schemes.

For more detailed information about the Programme, you can visit our website http://www.allianceindia.org/our-work/vihaan/

Details of Programme and users of software application

In India, People living with HIV (PLHIV) receive treatment support from Antiretroviral Treatment Center (ARTC) located at public health facilities. Once the PLHIV client is registered with ARTC, the clients are referred to Care and Support Centers (CSC) for other psycho-social support, adherence support, household follow-up services, etc. Monthly, information on the newly registered PLHIV clients and clients who need priority services is shared to Care and Support Centers for further follow-up. When the clients are referred to CSC for follow-up services, the clients are managed by the project coordinator at CSC, and the ORW provides field-level follow-up services.

Currently, the client management at Care and Support Centre is supported by web-based Client Management and Information System (CMIS), managed by the project coordinator and field-level outreach by Out Reach Worker through Tablet-based Mobile Application (eMpower) .The proposed RFP is for the Security Audit of these two applications, Web (CMIS) and Mobile Application (eMpower), under Vihaan.

Details of the Application:

S.No	**CMIS- Web Application**	**Details**
1	Operating System Details (Deployed Server)	Windows server 2019
2	Web/Application Server with version (	IIS
3	Front-end Tool (server-side Scripts)	ASP.Net
4	Back-end Database	MS-SQL
5	Site users (closed user group and / or open to public)	Closed User group
6	Levels of Authorization (number of roles)	Total 3 roles
7	Number of Dynamic pages	28
8	Provision for e-commerce and/ or payment gateway (Yes or No)	No
9	Whether the site contains any content management module (Y/N)	No

10	Is the web application is protected by a firewall/IDS/IPS/Load Balancer or any other security mechanism? Please provide details.	No
11	Are web services integrated with the application? If yes, how many?	Yes
II	**eMpower Application**	**Details**
1	Total screens	30
2	Data capturing screens	20
3	Data view screens	10
4	No. of user roles	3
5	No. of tables in the database	15
6	No. of fields	800 Apx
7	No. of APIs used	4
8	Web API	
III	**eMpower - APIs (Between Mobile and Web App)**	
1	No. of APIs	4
2	No. data capturing screens	3
3	Data view/ display	1 Report
IV	**eMpower – Web Content Management Website**	
1	Web API	4
2	Entry forms	3

Scope of work

1. Selected Auditing agency would be expected to perform the following tasks for website and web applications security to analyse and review the web application & mobile App security. The auditors will have to assess the vulnerabilities plates and rest that exist in applications through Internet vulnerability assessment and penetration testing.
2. This will include identifying remedial solutions and recommendations for implementing the same to mitigate all identified risks. The auditing agency will also be expected to propose a risk mitigation strategy and give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment. The mobile app and web application should be audited as per the National and International Industry standards and Govt of India approved measures. The auditor is expected to submit the final audit report after the remedies /recommendations are implemented. The final report

will certify the particular mobile app and web application as "Certified for Security". The scope of the proposed audit tasks is given below.

*The audit firm /company will be required to prepare the checklist/reports.

Task 1: Web security audit/assessment.

To check various web attacks and web/mobile applications for web attacks. The multiple checks/attacks/vulnerabilities should cover the following or any attacks vulnerable to web applications/mobile applications.

1. Vulnerabilities to SQL injections
2. CRLF injections
3. Directory Traversal
4. Authentication hacking/attacks
5. Identification and authentication failures
6. Password strength on authentication pages
7. Server-side request forgery (SSRF)
8. Scan JavaScript for security vulnerabilities
9. File inclusion attacks
10. Remotely exploitable vulnerability
11. Web server information security
12. Cross-site scripting
13. HTTP injection
14. Buffer overflow, invalid inputs, insecure storage etc.
15. Data encryption and confidentiality of data.
16. Cryptographic failures
17. Broken access control
18. Insecure design
19. Security misconfiguration
20. Vulnerable and outdated components
21. Any other vulnerable attack

Task2: Re-Audit based on the Recommendations Report from Task 1

The vendor will be responsible for providing a detailed recommendations report for the vulnerabilities observed in Task 1.

Task 3: Re-audit, if required, based on the Recommendations Report from Task 2.

If vulnerabilities are observed from the re-audit, the vendor must provide a detailed recommendations report on the vulnerabilities observed or found from Re-audit/Task 2. We expect that all vulnerabilities will be removed at the Task 3 stage.

The Audit firm must submit a summary compliance report at the end of each task. The final report should be separately certified that the mobile and web applications (should be mentioned the name of the mobile/web applications) are "Certified for Security".

After a successful security audit of the mobile and web applications, the security audit report from the auditor should clearly state that all web pages along with respective linked data files (in pdf/doc/xlsx etc. formats), all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said mobile/web applications.

Expected Deliveries

The auditing agency will be required to submit the following documents after the audit of each application (Mobile and Web). The audit form must also submit suggestions/recommendations and other detailed steps for enhancing security.

1. A summary and detailed report will be submitted with security status, discovered vulnerabilities and weaknesses, and misconfigurations with associated risk levels. The report will also mention necessary countermeasures and recommended actions for Risk mitigation.
2. All deliverables shall be in English language and in A4 size format.
3. The deliverables (like Summary compliance report, checklist, audit report executive summary and final compliance report after all observations) for each task to be submitted by the auditors for this assignment as mentioned in Task 1, Task 2)
4. Separate Security Audit Certification for Mobile and Web Applications and all associated components, including APIs

Criteria for the selection of agency:

Criteria	**Weighting %**	**Score**	**Weighted Score %**
Understanding of ToR Requirements	20%		
Value-Added Services and/or Innovations	10%		
Expertise/skills, have they demonstrated they have the relevant capabilities and experience to manage this project	30%		
Budget	25%		
Rationale timeline	5%		

Timeline:

The timeline should be proposed in consideration of all the tasks

Submission of Proposals

CERT – India empanelled agencies interested in carrying out the assignment are requested to submit their proposal per the details outlined below. The technical and financial proposals should be submitted separately.

The Technical Proposal should be concise and should address the following, at the minimum, without ambiguity: -

1. Brief Profile of Organization
2. Experience
3. Proposed security features.
4. References

Name of Project andClient	**Contract Value**	**Period of Activity**	**Types of Activities undertaken**	**References Contact Details (Name, Phone, Email)**

5. Detailed Project/Work Plan (as per the defined template)

Activity title	**Completion on/by**
1.	
2.	

The Financial Bid

The Financial Proposal should only indicate prices without any condition or qualification whatsoever. It should include all taxes, duties, fees, licensing, levies and other charges levied by Central & State, as may be applicable in relation to activities proposed to be carried out.

The technical and financial bids should be submitted in hard copy separately as “Technical Proposal” & “Financial Proposal” in the respective envelopes. Both these envelopes should be put in another bigger envelope mentioning the following:

Security Audit of Web (Client Management Information System) and Mobile Application (eMpower) under Vihaan Care and Support Programme

Interested agencies meeting the eligibility criteria must submit their technical and financial bids following the guidelines in our Procurement Portal (Tero Tam) on or before the closing date.

Interested Agencies can submit proposals through the Alliance India e-Procurement Portal. For this, the interested agency must first register with our e-procurement portal using the information below to share the details.

All supporting documents must be self-attested by the applicant organisation's consultant or Authorized Office Bearer.

The link to our e-procurement portal is https://evendor.terotam.com/user/signup.
Customer ID: - ZWAg9gZ6
Helpline No -9033053013

Queries regarding this RFP will be sent only to **procurement@allianceindia.org** latest by 03 April 2023 by 11.59 PM. Alliance India shall collaborate and respond to all meaningful queries from prospective applicants by 4 April 2023. Responses to questions shall be compiled and sent to all the applicants who raised the queries through email only.

The last date for submission is 06th April 2023.

Please get in touch with me on this email if you need any clarification.