REQUEST FOR PROPOSALS

Security Assessment Report (SAR) and Penetration Test in accordance with CMS Requirements and for Control Standards established by CMS known as Minimally Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 for Health-e-Arizona PLUS (HEAplus)

Responses Must Be Received By **August 14/2020 by Noon PST**

Table of Contents

Section I

The Center to Promote Healthcare Access, Inc. DBA Alluma

OUR STORY

We began as tenacious problem-solvers. In 1999, a group of changemakers from philanthropy and technology partnered to solve a problem: Why was California's Children's Health Insurance Program (CHIP) enrollment so low? Undeterred, they transformed California's CHIP application into a streamlined, effective, digital-only application. It worked, creating Health-e-App, the first application with an online signature for a public benefit program — reducing the application time from 97 to 7 minutes. Since then, we have connected millions of people to support and helped other changemakers at agencies and organizations realize our shared purpose.

OUR PURPOSE

We're on a bold mission to eliminate barriers to getting people connected to help, so that all people have access to support and services when they need it. By enabling our clients to better connect people with support, we make strides towards creating a system that leaves no one behind. When someone receives the support they need, their life transforms, creating a ripple effect on their families, communities, and the world. Our purpose is to create impact today while looking beyond the horizon for new ways to solve future problems.

Request For Proposal

Alluma is issuing this RFP for a Security Assessment Report (SAR) and Penetration Test in accordance with Centers for Medicare & Medical Services (CMS) Requirements and for Control Standards established by CMS known as Minimally Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 for Health-e-Arizona PLUS (HEAplus).

Your company is invited to respond to this RFP. Alluma will compare the competitive advantages that your proposal offers along with those from the other responding companies.

This RFP is not an offer to contract. Issuance of this RFP and the receipt of responses by Alluma does not commit Alluma to award a contract to any bidder.

Section II – Statement of Work

PURPOSE

The purpose of this request for Proposal is to procure security consultant services for Alluma on behalf of the State of Arizona (hereinafter referred to as Alluma) in order to conduct a Security Assessment Review (SAR) in the form and format required by the Center for Medicare and Medicaid Services (CMS) of the HEAplus eligibility and enrollment system. The final report must be provided in the CMS template found at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/Security-Assessment-Report-Template. The successful bidder should be familiar with MARS-E Version 2.0 requirements and controls as set forth by CMS and found at https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf. MARS-E 2.0 is a compendium security framework but largely follows FISMA Moderate standards and HIPAA security and privacy protocols.

The SAR is a multi-week assessment expected to include interviews, document review and IT evidentiary audits to evaluate the HEAplus program's compliance with MARS-E, Version 2.0 (MARS-E V2) compliance. HEAplus is Arizona's online eligibility application and determination system for Medical Assistance, Nutrition Assistance and Cash Assistance which is moving from on premise operations to cloud operations which requires an update SAR.

In addition to the SAR, the security consultant is to conduct Penetration Tests (PenTests – external and internal) and is to also include vulnerability testing on HEAplus.

OVERVIEW

As per CMS, MARS-E V2 requirements, a SAR is to be conducted by an independent third-party assessor. The purpose of this SAR is to conduct an assessment of the security controls in the HEAplus system and associated policy, processes, operations and technology, and security protocols every three-hundred-sixty-five (365) days, or when there is a significant change in the system. A SAR was recently completed in June of 2020 however, a new SAR must be conducted as HEAplus is moving to the cloud in late October. The SAR is to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Given this SAR will be completed prior to the implementation of HEAplus in the cloud, the security consultant will be required to review the "Planned" controls in the non-production environments to determine if the planned control, if implemented in Production as it has been implemented in the lower environment (User Acceptance Testing environment) would meet the requirements of the MARS-E V2 control. Likewise, the Penetration tests will be conducted in UAT (User Acceptance Test) environment as well.

SECURITY CONSULTANT MINIMUM QUALIFICATIONS

The security consultant must meet at least the minimum qualifications as listed below:

- Be independent of the State of Arizona (no ongoing services) Administrative for Health Care Cost Containment Services (AHCCCS) and Department of Economic Security (DES).
- Certified Information Systems Auditor (CISA) or equivalent.
- Experience completing at least three (3) States or Federal Agency MARS-E V2 SAR audits or FISMA Moderate and HIPAA SAR equivalent audits.
- Demonstrated knowledge and experience in conducting SAR audits under MARS-E V2.
- Three (3) years of Penetration Testing and vulnerability assessment conducted by a person who has an OSCP certificate or equivalent.

CONTRACTOR RESPONSIBILITIES/TASKS/SCOPE OF WORK

For this Request for Proposal (RFP), the security consultant shall:

- Conduct an Assessment Security Test (i.e., vulnerability testing and penetration testing) and evaluation of HEAplus within its ACA accreditation security boundary to obtain an accurate representation of the information system security controls that pertain to these systems and the associated technical integration represented in these systems technical architecture. One hundred percent of the MARS-E V2 controls are included in the scope of this SAR and PenTests. This Assessment must include identification of the issues or vulnerabilities identified, assignment of a risk level (e.g. critical, high, medium, and low), identify the MARS-E control(s) associated with the vulnerability and provide remediation recommendations for resolving the vulnerability identified.
- Provide an agreed to The Rules of Engagement created during the engagement kickoff meeting including the timeline, locations, evidence handling procedures, constraints, communication and escalation plan, and permission to test.
- Identify security weaknesses whether found from the PenTests or SAR and provide recommended remediation / mitigation.
- As part of the SAR, conduct an architectural and operations security review of HEAplus “planned” Cloud controls in the UAT environment to determine if implemented as done in UAT if the planned control would be compliant with MARS-E V2 when in Production.
- As part of the SAR, conduct an assessment of the implemented Cloud controls in the UAT environment to determine if they are unchanged that they would be compliant with MARS-E V2 in Production.
- As part of the SAR, conduct and assessment of any POA&M open with CMS to determine that the milestones are being met and the control remediation is progressing as expected and reported to the State of Arizona and CMS.
- Develop or validate a data flow map between all the HEAplus and the interconnected systems
- Conduct a full data inventory for HEAplus, with particular attention to what CMS defines as Medicaid data.
- Review the following artifacts submitted to the State of Arizona and CMS for the purpose of insuring that the SAR and PenTests results are consistent with information submitted:
    - HEAplus (Alluma) Plan of Action & Milestones (POA&Ms)

  - HEAplus (Alluma) Security Risk Assessment
  - HEAplus (Alluma) Information System Security Plan (SSP)
  - HEAplus (Alluma) Interconnection Security Agreement (ISA)
- Review and evaluate the HEAplus (Alluma) Policies and Procedures for the HEAplus Cloud environment to insure they have been appropriately updated and communicated regarding this cloud move.
- All findings should include the calculated CVSS score along with the rationale behind the score.
- At a minimum, the PenTests for the HEAplus UAT cloud environment shall:
  - Be performed on HEAplus;
  - Identify network and identified vulnerabilities;
  - Include network and device scans;
  - Include and execute a detailed attack plan shall be developed using the information gathered during reconnaissance and scanning. [Note: The attack plan shall be followed to gain access and maintain access to systems through exploited vulnerabilities. Evidence must be collected at each stage of the attack plan to demonstrate if the security consultant is able to penetrate the network and systems.]
  - Develop a comprehensive remediation plan based on the ranking and prioritization of the vulnerabilities exploited, if any.
- The security consultant shall work closely with Alluma, and where appropriate, the HEAplus Project Director from AHCCCS throughout the assessment, reporting results regularly so that Alluma and the State of Arizona are informed of progress and issues in a timely manner.
- Conduct a planning meeting with Alluma management to discuss key business operations and management's understanding of criteria. This information will assist them to determine that such criteria are comprehensive, objective, and complete by discussing key business operations and services provided by Alluma.
- Gaps and or issues discovered during the SAR or PenTests shall be reported in the following manner:
  - In real time, as exceptions are identified;
  - In periodic status meetings with Alluma and the State of Arizona HEAplus Project Director;
  - In the PenTests detailed results draft;
  - In the PenTests detailed final Report;
  - In the draft Security Assessment Report; and
  - In the final Security Assessment Report in a format acceptable to the State of Arizona and CMS – see template provided from CMS. [Note: This SAR will not be considered final until it is accepted as complete by CMS.]

ASSUMPTIONS

The following assumptions have been made in defining the statement of work.
Changes to these assumptions may require a corresponding change in scope. The security consultant will receive full and timely cooperation from all members of the Alluma teams which

includes, but is not limited to, Alluma's good faith and timely provision of any information and resources reasonably requested by the security consultant in connection with performing the SAR and PenTests of HEAplus.

PROJECT DELIVERABLES with TIMEFRAME/DUE DATES

The security consultant responsibilities listed above shall be performed and completed by 10/02/2020. The RFP deliverables shall include a comprehensive SAR in the CMS Template submitted in draft to Alluma and the State of Arizona HEAplus Project Director and the final SAR as approved and accepted by CMS. The PenTests results in draft and final shall also be provided to Alluma and the State of Arizona HEAplus Project Director.

It is expected that the security consultant provides recommendations to improve the overall risk posture of the environment within scope including, but not limited to, policies, procedures, patching, professional services, and compliance.

The PenTests documentation shall include, at a minimum:

- A list of identified critical and high severity vulnerabilities by host/IP for each network segment including the vulnerability classification, reference material, CVSS score, details of the type and nature, and remediation recommendations. An additional vulnerability scan document shall be provided that includes all severity level vulnerabilities by host/IP with the same details as above.
- A list of exploited vulnerabilities by host/IP for each network segment including the vulnerability details, methods used to exploit the vulnerability, screenshots of any evidence collected, and remediation recommendations.

PROJECT WRAP-UP AND REPORT DEVELOPMENT

The security contractor shall provide written status report and finding weekly on all high and moderate risk findings. Draft deliverables for the SAR and PenTests results shall be presented to the Alluma and the State of Arizona HEAplus Project Director. Upon review of and approval of the draft documents by Alluma and the State of Arizona HEAplus Project Director, the deliverables will be converted to PDF format and sent to the HEAplus Project Director for their submission to CMS (on or before 10/2/2020). If CMS does not accept the submitted documentation for any reason, the security consultant will be responsible for amelioration of the submission until it is accepted by CMS.

The security consultant shall retain all documents in a secure file repository, where they are to reside for ninety (90) days post CMS acceptance of the SAR, at which time the repository will be decommissioned. The security consultant shall advise Alluma of their decommissioning.

Section III – General Terms & Conditions

Electronic response, submit your response electronically via email to Sandra Mowry, Alluma Procurement Officer, at Procurement@alluma.org Subject line of your response email needs to read: "RFP for HEAplus Security Assessment Report and Penetration Test" along with your company's name.

Proposal Costs. Costs for developing proposals are entirely the responsibility of the proposer and shall not be charged to/or otherwise reimbursed by Alluma

Proposal Becomes Alluma's Property. The RFP and all materials submitted in response to this RFP will become the property of Alluma. Do not submit anything considered "proprietary" or "confidential"

Questions and Responses Process. Submit all questions relating to this RFP to Sandra Mowry at Procurement@alluma.org

All questions must be received no later than 12:00 PM. PST on August 4th, 2020.

Alteration of Terms and Clarifications. No alteration or variation of the terms of this RFP is valid unless made or confirmed in writing by Alluma. Likewise, oral understandings or agreements not incorporated into the final contract are not binding to Alluma.

If a proposer discovers any ambiguity, conflict, discrepancy, omission, or other error in the RFP, the proposer must immediately notify Alluma of such error in writing and request modification or clarification of the document. If a proposer fails to notify Alluma of an error in the RFP prior to the date fixed for submission, the proposer shall submit a response at his/her own risk, and if the proposer enters into a contract, the proposer shall not be entitled to additional compensation or time by reason of the error or its later correction.

Modifications or clarifications to the RFP might be made in a case by case requirement and electronically submitted to all Proposers.

All modifications or clarifications will be received and resolved no later than 12:00 PM PST on August 10th, 2020.

Incomplete Proposals May be Rejected. If a proposer fails to satisfy any of the requirements identified in this RFP, the proposer may be considered non-responsive and the proposal may be rejected.

Late responses will not be considered

Section IV – RFP Procedure

SUBMISSION OF PROPOSAL

The security consultant is to provide the following to be considered a successful offeror to this RFP:

- Cover Letter, including:
  - Company name and contact number.
  - Signature of authorized company representative.
  - Name and contact information of person responsible for response to this RFP.

- Company experience that meets the required minimums to bid on this RFP (Limit 5 pages)

- Company Methodology and Approach (Limit 10 Pages), including proposed methodology and approach that details the processes your firm will utilize to complete the Scope of Work requirements. Capacity/Availability of the firm to initiate services within specified project timelines;

- Timeline and Staffing (Limit 3 pages – Resumes are not included in this limit) for completion of this project on time.

- Identification of key project members and their experience and approach to meeting the requirements of this RFP.

- Pricing, which is to include:

  - Provide an all-inclusive overall project price for performance of the services listed in the above Scope of Work. Pricing shall be broken down by SAR and PenTests. The lump sum pricing for each phase shall include costs associated with Project Deliverables and Project Wrap-Up as described in this RFP.
  - Pricing should include rate per hour, staff hours proposed, travel (unlikely) or other costs and total cost by SAR and PenTests.
  - Identify key assumptions to meet the required timeline and pricing proposed.
  - Please submit your best and final pricing.
  - It is the security consultants' responsibility to monitor project costs and to remain on budget.

Please submit your response electronically via email to Sandra Mowry, the Alluma Procurement Officer at Procurement@alluma.org

EVALUATION CRITERIA AND AWARD

Responses will be evaluated based upon the evaluation criteria listed below. The evaluation factors are listed in their relative order of importance, include:

- Experience of Company and Personnel
- Method and Approach
- Timeline
- Cost

Alluma will evaluate responses and will award the RFP to the Offeror with the most advantageous response(s) based upon the evaluation criteria set forth above.

The awarded security consultant shall safeguard all information regarding this RFP as confidential. The security consultant shall establish and maintain procedures and controls, pre-approved by Alluma, for the purpose of assuring that information contained in its records or obtained while carrying out the scope of work for this RFP shall not be used or disclosed, except as required to perform duties under this contract.

RESPONSE TIMELINE: RFP Response Due 8/14/2020 at NOON Pacific Time

PROJECT TIMELINE: Upon State of Arizona Approval which is expected the week of 8/17/2020 and must be completed by 10/02/2020.