Request for Proposal

CRISP Shared Services (CSS)

All final responses are due no later than 6:00pm ET (Eastern Time) on December 20, 2022

Comprehensive Annual Security Audit

Request for Proposal – "RFP"

TO ALL PROPOSERS

You are invited to submit a Proposal to explain your solution for a comprehensive annual security audit that will include a System and Organization Controls 2 (SOC 2 Type 2), HIPAA/HITECH, COMAR (Code of Maryland Regulations) audit, cybersecurity testing, and validated HITRUST assessment of a health information exchange (HIE). The audit will evaluate adherence to HIPAA/HITECH and COMAR (10.25.18) requirements for security and privacy, as well as the controls required for HITRUST Common Security Framework (CSF) compliance. You will need to describe how your solution will meet CRISP Shared Services' (CSS) requirements as described herein. All Proposals should be submitted electronically to:

bezawit.sumner@crisphealth.org

1. Intent to bid on this proposal must be submitted by November 18, 2022, at 6:00pm ET
2. Questions from potential vendors are due by November 30, 2022, at 6:00pm ET
3. Responses to Questions will be provided on or before December 07, 2022
4. Final Proposals must be received no later than 6:00pm ET on December 15, 2022

If you have any questions about preparing your Proposal, please contact us.

Contact Info

Name: Bezawit Sumner
Email: bezawit.sumner@crisphealth.org

Please note that this Request for Proposal letter does not constitute a guarantee on the part of CSS that a contract will be awarded. No payment will be made for costs incurred in the preparation and submission of a Proposal in response to this Request for Proposal.

THIS IS NOT AN ORDER OR A CONTRACT

Table of Contents

1. Background and Overview

The purpose of this solicitation is to obtain an audit firm to assess whether patient data is processed, transmitted, and stored by the HIE and its vendors in a secure manner and in accordance with the Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health (HITECH), and State level requirements defined within the Code of Maryland Regulations (COMAR) 10.25.18 to minimize the potential for unauthorized disclosure or breach of protected health information (PHI), and HITRUST CSF compliance.

CSS is formally designated as Maryland and D.C.'s statewide Health Information Exchange ("HIE") and is incorporated as a non-profit entity charged with the mission to advance health and wellness of patients throughout Maryland, the District of Columbia, West Virginia, Connecticut, and Alaska by enabling healthcare providers to share clinical data with other hospital systems, providers, and stakeholders across the Region.

CSS is committed to providing secure operations and protection of private health data. As a Health Information Exchange, compliance with HIPAA/HITECH and COMAR is a business requirement. With or without HIPAA compliance, the security and privacy of the data made available by CSS on publicly accessible websites and through the numerous custom developed applications running on them is a high priority.

2. Minimum Requirements

The successful Offeror will be a Certified Public Accounting firms (CPA) firm with expertise in conducting audits of HIEs (health information exchanges), health care facilities, business associates, providers, and/or employers, in Maryland and/or other states, as well as being a certified HITRUST assessor. The firm must be experienced in developing qualitative reports and recommendations that provide unified reports on all audit findings and must document the ability to meet reporting deadlines. Audits conducted by the successful Offeror will be performed in accordance with auditing standards generally accepted in the United States of America and Government Auditing Standards, issued by the Comptroller General of the United States. The Offeror should include an organization chart and descriptions of selected audit projects or programs that the Offeror successfully performed for other clients involving services similar to those requested by this RFP (request for proposal).

The successful Offeror will conduct an annual information technology security audit of the State-Designated HIE to review controls designed to ensure electronic health data is processed, transmitted, and stored by the HIE and its vendors in a secure manner and in accordance with HIPAA, as amended by HITECH, and State level requirements defined within COMAR 10.25.18 to minimize the potential for unauthorized disclosure or breach of PHI. (See Health General § 19-101, et seq., Annotated Code of Maryland, and COMAR 10.25.10, Maryland Trauma Physician Services Fund and COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information.) The Offeror will also incorporate the required assessment procedures to conduct a validated HITRUST assessment of CSS.

The audit must utilize cybersecurity testing procedures, including vulnerability scanning and social engineering procedures, to evaluate if data is adequately protected from unauthorized access through the

exploitation of system vulnerabilities or security weaknesses. A SOC-2 Type 2 report, COMAR and, HIPAA/HITECH report and validated HITRUST assessment should be outputs of the engagement.

The auditor will develop a plan that consists of at least the following activities as part of the annual audit:

- Planning/identifying the audit scope, objectives, and detailed procedures for conducting the audit in conjunction with CSS
- Timeline for completion of audit activities/deliverables
- Kick-off meeting with CSS and a representative of the MHCC
- Weekly status meetings with CSS (primarily during field work)
- Follow-up on the status of corrective actions implemented from the previous audit
- Completion of a formal report detailing audit findings and observations as well as recommendations for mitigating risks identified
- Exit meeting with CSS and their Audit Committee members

The annual audit of the State-Designated HIE must adhere to standards that provide sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions for the audit period under review, which will be April 1, 2022 – March 31, 2023, and HITRUST validated certification submission date of October 2023. The audit must be based on tests and samples considered necessary to report on the findings and conclusions arrived at within the context of the audit objectives. The final report should include a summary of the audit scope, objectives, methodology, findings and conclusions, recommendations, summary of the views of responsible officials, and as appropriate, the reason for any confidential or sensitive information omitted. The SOC-2 Type 2 audit methodology must include at a minimum the following activities:

1. Conduct interviews with HIE's key personnel and management and its subcontractors, as applicable.
2. Review relevant criteria and best practices, including federal and State laws and requirements, the HIE's policies and procedures, and its subcontractors' policies, procedures, and Service Organization Control (SOC) audit reports.
3. Conduct interviews and review documentation related to HIE's oversight and monitoring of its subcontractors.
4. Review policies, procedures, and guidelines related to the security of the HIE's participants' patient data to ensure adherence with HIPAA, HITECH and COMAR requirements and establish criteria and guidelines applicable to all audit procedures performed.
5. Perform tests and observations of system and process controls designed to ensure the HIE's participants' patient data is processed, transmitted, and stored in a secure manner, including security configurations, password settings, procedures for monitoring security such as logging, log reviews, system alerts, oversight, and training activities.
6. Review change management processes and procedures and documentation artifacts for changes implemented during the audit period to confirm that appropriate procedures were followed in accordance with policies, procedures, and contractual requirements.

7. Review, test, and assess the HIE's and its subcontractors' procedures for granting, modifying, and removing user access to systems and applications including reviewing access request and authorization documentation for user accounts, comparing lists of users to lists of current and terminated employees and contractors, and testing last login and last password change dates.
8. Review corrective actions performed by the HIE and assess the status of the previous audit findings and recommendations.
9. Review and observe physical and environmental controls for the HIE, including walkthroughs during business hours and after normal business hours.
10. Perform internal and external scans of the HIE's servers and network devices to identify critical, high, medium, and low vulnerabilities.
11. Perform vulnerability scans of HIE's web applications.
12. Perform social engineering procedures, including email and phone phishing and planting USB devices, as applicable and feasible.
13. Follow up on the status of corrective actions from prior year audit findings and assess the effectiveness of the corrective actions performed by the HIE.
14. Develop recommendations for improvement of controls based on audit findings and conclusions.

Appropriate testing and evidence gathering will also be conducted as required to complete a validated HITRUST assessment. Steps required for the Interim Re-assessment must also be completed if the offeror intends to bid on this option.

Responses that will be graded as "Conforming" and "Complete" should demonstrate an auditor's experience and capabilities to performing a healthcare security and privacy controls audit, according to the Scope Requirements defined in a following section, and a set of quotes specifying the charges for deliverables.

3. Response Format

CSS discourages responses that are merely marketing collateral and so brochures or other presentations – beyond those sufficient to present a complete and effective proposal – are not desired.

Unless specified below, CSS will not impose a page limit to proposals or required sections. CSS does encourage proposals to be concise and of succinct length.

Please NOTE: All responses, assertions, and commitments made in this proposal will be part of any contract.

The response should include the following sections:

Response Section	Title	Format
A	Cover Letter	Letter on company letter head signed by representative with legal contracting capacity. Appropriate company contact information must be included. No more than 2 pages.
B	Table of Contents	
C	Executive Summary	No more than 3 pages.
D	Response to CSS Requirements	Pages as required. Please remain concise.
E	Response to General Questions	Pages as required. Please remain concise.
F	Appendices	
P1	Contact Information for Previous/Existing Customers (to serve as a Reference)	Pages as required.
P2	Project Staff Resource Resumes	Pages as required.
P3	Pricing Spreadsheets	Pages as required.
P4	Acceptance of Terms	Executed copy of Acceptance of Terms document included in RFP. Pages as required.
P5	Standard Contract	Copy of your company's standard contract. Pages as required.

4. Executive Summary Guidelines

CSS requests up to three (3) pages for an Executive Summary. The summary should introduce a responder's company, any relevant offerings, and should provide a summary of the response.

5. Response to CSS Requirements

To ensure that the proposal can meet CSS's specific needs, each response should address the specific requirements listed below. Each discussion should include a description of how the proposal will meet each specific requirement. Responses will be scored based on how the proposal specifically addresses each individual requirement.

Please feel free to include explanations, caveats, conditions, or other information that will help qualify or explain your answers. Please also include any additional cost that may be incurred by CSS above and beyond the proposed pricing quoted.

Please NOTE: All responses, assertions, and commitments made in this proposal will be part of any contract.

Please NOTE: If specific additional costs are not included in the use case discussion, CSS will assume the cost to implement and run the use case is part of the overall pricing proposal.

Scope

This security assessment covers the execution of an annual security and privacy audit, in accordance with HIPAA/HITECH and COMAR regulations, the preparation of a SOC-2 Type 2 audit report addressing specifically Security, Confidentiality, and Availability with the option to include Privacy and Process Integrity: a validated HITRUST assessment, and the option for a HITRUST Interim Re-assessment. In addition, the annual security audit will cover vulnerability assessment, web application assessment, and social engineering requirements, as specified in the requirements section.

Deliverables

The Auditor will deliver a SOC-2 Type 2 report which adheres to AICPA standards, and details the methodology used, findings of the examination, and which documents recommended actions for improvement, a HIPAA and HITECH assessment report and as well as the completion of a validated HITRUST assessment (and Interim Re-assessment where applicable).

6. General Questions

CSS requests responses to all questions listed below, and all answers should either be clearly provided within the context of the proposal and/or in their own separate section. All answers provided should be succinct in length to ease reviewer evaluation but should take care to answer each question in all necessary and appropriate depth.

CSS will assume that any non-answer will indicate that any proposed company or technology will be unable to provide or unwilling to disclose a solution to the question, and this may negatively impact CSS's perception of the overall proposal. Inability to provide a response to any question will not immediately disqualify a proposal from consideration.

Please NOTE: All responses, assertions, and commitments made in this proposal will be part of any contract.

1. What is your company's Dun and Bradstreet number?
2. Where is your company headquartered?
3. How long has your company been in business?
4. How many employees work for the company?
5. Is the company privately held or publicly traded?
6. Please note any relevant accreditations your organization has achieved.

7. To fulfill the requirements of this RFP, will you rely on any partnerships, subcontracts, or other relationships? If yes, please describe the role the subcontractor will play and any other salient HIEs?
8. Have you completed SOC-2 evaluations on other HIEs?
9. Please describe your work with other HIEs, if any. In your work with HIEs, like CSS, do you rely on any partnerships, subcontracts, or other relationships? If so, please explain.
10. What is the standard timeline for completing the type of work described in this RFP?
11. Please describe your approach to cybersecurity testing/social engineering testing.
12. Please describe your experience with HIPAA/COMAR 10.25.18.
13. Can you provide a redacted SOC-2 you completed?
14. Are you a certified HITRUST assessor?
15. Have you completed validated assessments and interim re-assessments under HITRUST for other HIEs?
16. Have you coordinated and completed a SOC-2 Type 2 audit ***AND*** validated HITRUST assessment for other clients?
17. If so, what is the typical timeline for engagement with the client?
18. If so, how does your company minimize the impact on the client as you leverage the evidence requested to fulfill the needs of both tracts of work?

7. Full Pricing Proposal

CSS requires a pricing proposal to understand the total cost of your services. Outline your financial proposal in an Excel spreadsheet and include it as *Section P3* in your response. Include total expected cost with a detailed breakout of separate cost areas. Pricing for optional engagements in Years 2-3 strongly preferred.

Please document any other costs that CSS may incur in doing business with your company in this area of work. Also include the hourly expense for each resource type that may be engaged in this effort.

Responses should include a timeline for completing the testing and ANY potential cost CSS may incur.

Please include a copy of your standard contract with this proposal.

Please NOTE: All responses, assertions, and commitments made in this proposal will be part of any contract.

8. Evaluation

CSS will evaluate each proposal for completeness and will score the proposals based on the understanding that any proposed solution will effectively meet the requirements set forth in this RFP. CSS's scores will be kept confidential and will not be disclosed to responders. Consideration may focus on, but is not limited to, the following:

- Adequacy and completeness of the proposal
- Demonstrated understanding of penetration testing specific to CSS's environment
- Experience and demonstrated competence in providing like services
- Quality of proposed approach
- Cost
- Timeline to complete

The order of these factors, above, does not denote relative importance.

CSS reserves the right to:

- Select for contract or for negotiations a proposal other than that with lowest costs.
- Accept/Reject all proposals or portions of proposals received in response to this RFP, to make no award, or to issue a new RFP.
- Waive or modify any information, irregularity, or inconsistency in proposals received.
- Request modification to proposals from any or all contractors during the review and negotiation.
- Negotiate any aspect of the proposal with any individual or firm and negotiate with more than one individual or firm at the same time.

9. Bidder's Instructions

To be considered, all proposals must be submitted in writing and electronic format and must respond to the items outlined in this RFP using the requested format. CSS reserves the right to reject any proposals that are, in the sole judgment of CSS, non-responsive or non-conforming. Responses to this RFP should be complete but concise.

CSS is not a state entity nor is the organization bound by state procurement guidelines and regulations. CSS does encourage Minority Business Enterprise (MBE) designated entities with relevant solutions to respond to this solicitation.

10. Modifications

Any changes, amendments, or modifications to a proposal may be submitted by email but will not be considered acknowledged until a response email from CSS indicating receipt and acceptance of the

modification is received. CSS reserves the right to request clarification and/or further technical information from any contractor submitting a proposal.

11. Request for Proposal (RFP) Terms and Conditions

Proposal Response

CSS reserves the right to reject any/all proposals received in response to this RFP. Any information obtained will be used, along with other information that CSS deems appropriate, in determining suitability of proposed offer. Bidders whose proposals were not accepted will be notified that a selection is made, or if it is decided, that no proposals are accepted. CSS has no obligation to explain the basis of or reasons for the decision it makes relating to the proposals and/or this RFP. CSS may identify multiple bidders who are determined suitable and negotiate with each of them on parallel tracks, pending a final contracting decision. Any proposal failing to meet all requirements may be eliminated from consideration and declared not accepted.

Proposal Becomes CSS' Property

All proposals become the property of CSS and will not be returned to bidders.

Formal Contract

A bidder receiving a positive response to their proposal should be prepared to immediately begin negotiation of final terms based on the RFP and other mutually agreed terms and conditions, if terms described by bidder in their response may be rejected in whole or in part and/or otherwise negotiated by CSS in the contracting process. In addition, a positive response from CSS does not assure a bidder that a contract will be entered; CSS may discontinue negotiations with a bidder at any time, in its sole discretion. PLEASE PROVIDE A COPY OF YOUR STANDARD CONTRACT DOCUMENTS WITH YOUR SUBMISSION**.**

Within 5 days of receiving a positive response, the bidder will be expected to notify CSS in writing of its contract team, which shall include the individual with authority to approve and execute any final legally binding agreement with CSS.

Until and unless a formal contract is executed by CSS and bidder, CSS shall have no liability or other legal obligation to bidder whatsoever, relating to or arising from this RFP, the RFP process, decisions as to awards resulting from this RFP, or otherwise.

In no event will CSS be responsible for damages or other remedies, at law or in equity, arising directly or indirectly from its decision on the award of the PDMP (Prescription Drug Monitoring Program) contract or for any action taken or not taken in response to or because of this RFP or bidder's response.

Maintaining Pricing

Prices must remain valid for at least ninety (90) days from the Closing. Contract negotiations will include price re-verification if the price guarantee period has expired. CSS reserves the right to request that a bidder only provide a portion of the proposed deliverables or exclude certain partners. If bidders are

unwilling to comply with RFP requirements, terms and conditions, objections must be clearly stated in the Cover Letter to the proposal.

Cost of Proposal Preparation

All bidder's costs of proposal preparation and any negotiation will be borne by the bidder.

Applicable Law

The Laws of the State of Maryland shall apply, except where Federal Law has precedence. The successful individual or firm consents to jurisdiction and venue in the State of Maryland.

By the signature of its authorized representative, Bidder acknowledges that it understands and accepts the terms of this RFP and intends to bid on this project.

BIDDER: _____

By: _____

Title: _____

Date: _____