VERMONT INFORMATION TECHNOLOGY LEADERS

REQUEST FOR PROPOSAL

FOR

Identity Access Management and API Security Platforms

ISSUE DATE: April 4, 2023

RESPONSE DATE: May 3, 2023

Table of Contents

Contents

Request for Proposal for Identity Access Management and API Security Platforms

Introduction

Vermont Information Technology Leaders, Inc. (VITL) is seeking written proposals from firms with deep experience designing and implementing Identity Access Management and API Security Management platforms. We are looking for a strategic advisor with extensive healthcare interoperability and FHIR experience to help design, specify, acquire and implement these platforms. Bidders are also asked to describe their approach to providing ongoing services related to development, integration, maintenance, and support of these platforms.

About VITL

VITL is legislatively designated to operate the Vermont Health Information Exchange (VHIE), a secure, statewide data network that gives health care organizations in Vermont the ability to electronically exchange and access their patients' health information in order to improve the quality, safety, and cost of patient care.

VITL collects, matches, and standardizes patient data from health care organizations across the state, including hospitals, primary and specialty care providers, Federally Qualified Health Centers, home health providers, nursing homes, commercial labs, and others.

The data is made available to stakeholders, including participating health care organizations, to inform providers' point-of-care decisions; to OneCare Vermont and the Vermont Blueprint for Health for their work to improve and reform care; and to the Vermont Department of Health to support public health efforts in service of all Vermonters. VITL creates ways for providers to securely access the data about their patients that is in the Vermont Health Information Exchange. VITL services include a secure web portal for looking up patient information, integration with some electronic health records to enable providers to see everything they need in one place, and behind-the-scenes delivery of over 1.4 million clinical messages a year in the form of laboratory results, radiology reports, and transcribed reports.

VITL Point of Contact

The sole point of contact for this RFP is listed below. Reaching out to anyone other than the primary point of contact for this RFP could be a reason for disqualification.

Heidi Banks, Business Operations Manager
RE: Identity Access Management and API Security Platforms
Vermont Information Technology Leaders, Inc. (VITL)
hbanks@vitl.net

Pertinent Dates

You may contact the VITL point of contact for any additional needs to assist you in preparing your response.

Deadline for vendors to submit proposals: May 3, 2023, at 5pm Eastern. Submit your proposal via email to the VITL point of contact at the email address provided.

Correspondence: Any correspondence including proposals submitted should be directed to the VITL point of contact at the email address provided. To ensure timely processing of correspondence, please begin the subject line with "Identity Access Management and API Security Platforms".

Deadline for questions: All questions must be submitted to VITL's point of contact by April 12, 2023, at 5pm Eastern Time.

VITL response to questions: VITL's response to all questions will be sent by April 19, 2023, at 5pm Eastern Time.

Vendor Selection: VITL anticipates selecting the finalist vendor by June 7, 2023, at 5pm Eastern Time.

Project Objective

This project's main objective is the design and implementation of Identity Access Management and API Security Management platforms. These platforms are intended to become part of VITL's enterprise architecture with responsibility for ongoing maintenance and support shared between the Bidder and VITL. VITL will consider both fully hosted solutions (solutions developed and sold directly by the Bidder) or will partner with the Bidder to license and configure 3rd-party SaaS, IaaS, and PaaS solutions.

Project Scope

The following are the high-level platform goals in scope for this RFP. Responses should specifically address the design and implementation of the following:

General Requirements

- Identity Access and Management - The IAM solution should allow VITL to provide identities and configure role-based access and support federated identities and single sign-on. It must support MFA/2FA and a robust set of authentication and authorization mechanisms, such as OAuth2.0, OpenID Connect, JSON Web Tokens, SAML, and Web Service Federation.
- API Security - The API Security solution must offer robust security measures to protect against the OWASP Top 10 API Threats. Responses should describe the platform's internal capabilities for real-time security and compliance, as well as any other manual options for validating security and compliance of APIs through regular code review and/or penetration testing.
- Extensibility/Scalability – Responses should consider how VITL can cost-effectively implement a baseline environment while also being assured the solution is readily extensible and scalable to meet anticipated future needs. Responses should describe the pricing model for extending the platform so VITL can anticipate future costs.
- High-Availability and Continuity - Responses should provide a design that supports high availability, minimal to no downtime for patching and maintenance, and geographic redundancy.

Proposal Details

System Architecture

The proposed architecture should be cloud-based, and all systems and data storage must reside in the United States. In the case where Bidder is also the solution provider, the proposal should include detailed price breakdowns of the recommended platform(s). If the Bidder is proposing 3rd-party tools or services, the proposal should include detailed cost estimates of those tools or services.

Where applicable, include the following details in your response:

- Pricing or cost estimates for all SaaS, PaaS, or IaaS applications, tools, or services employed in the solution
- Details of the virtual system compute, memory storage requirements, SaaS applications, tools, or services
- Diagrams showing system component inter-relationships and network communications

Design, Implementation and Support

The parties involved in the design, implementation and ongoing support aspects of this proposal must have extensive healthcare interoperability and FHIR experience. All work performed on this proposal must be conducted by individuals located in the United States.

Include the following details in your response:

- Pricing for the design, configuration, and implementation of the baseline IAM/API Management platform
- Overview of your firm's approach to business analysis and systems design
- Overview of your firm's relevant healthcare and FHIR experience which will ensure the successful implementation of the potential future use cases described below
- An anticipated timeline for installation and configuration of the baseline platform
- Pricing for one year of maintenance and support renewable annually for a period of up to three years
- Documented SLAs for incident resolution
- Hourly rates for ongoing development and integration services

Potential Future Use Cases

In framing your response to this RFP, please consider the following potential future use cases. Although these future use cases are not explicitly part of the pricing or scope of work in this proposal, the Bidder is asked to describe their approach to designing, estimating and implementing projects of this type utilizing, or extending, the baseline infrastructure bid in this RFP.

API Gateway integration with a backend FHIR R4 API

- Provide a secure API endpoint over the SMART App Launch Framework to connect client applications to VITL's backend FHIR R4 API. The client-side would be a SMART on FHIR application, launched from inside a client hospital's Electronic Health Record (EHR), which retrieves and displays various data elements from the backend FHIR API (e.g., Quality Indicators, Procedures, Conditions, Labs, Radiology, Vaccinations, and Medications). The respondent's role in this project would be to work in collaboration with VITL's vendors and clients to design, integrate, and develop code in support of secure connectivity between the client app and backend infrastructure.

- Provide a secure API endpoint for Vermont residents to access to their health information in accordance with the Office of the National Coordinator for Health Information Technology (ONC) 21st Century Cures Act and the Centers for Medicare and Medicaid Services (CMS) interoperability rules. This API will support patients' access to their health record through 3rd party applications. In addition, we intend to consider integration with the State of Vermont's existing identity and authorization solutions, allowing end-users to enjoy a single sign-on experience with other State services.
- Provide a secure API endpoint over the SMART on FHIR framework to collect patient generated data, either directly from remote patient monitoring tools or via a patient's mobile application. This data, which could include health history, device data, or patient-reported outcomes, would then be securely shared with health care organizations to provide a more comprehensive picture of a patient's ongoing health.

Single Sign-On to VITL's web-based Provider Portal

- Provide single sign-on to VITL's Provider Portal from inside a health care organization's Electronic Health Record (EHR). The EHR user would request a patient's chart by selecting a link or button from within the EHR application. The patient's chart from the Provider Portal would then be opened in the client's system's web browser, using the EHR user's credentials and identity. The respondent's role in this project would be to work in collaboration with VITL's Provider Portal vendor to design, integrate, and develop the single sign-on functionality with a variety of VITL's clients.

Project Expectations and Responsibilities

At the conclusion of this RFP process, VITL anticipates the following immediate next steps with the selected Bidder:

- Finalization of an implementation plan for the baseline infrastructure scoped in this RFP
- Procurement/licensing of any services, applications, or tools which were either quoted directly by the Bidder from the Bidder's own SaaS offering(s), or which were estimated by the Bidder for recommended 3rd party SaaS, PaaS, or IaaS solutions
- Implementation of the baseline platform scoped in this RFP

In the future, VITL intends to scope services related to the potential platform use cases outlined in this RFP. That work would include:

- Business analysis and systems design
- API configuration, development, or integration services
- Single sign-on configuration and integration services

VITL will rely on the selected Bidder for all systems installation and configuration defined in this scope, as well as development and integration of future use cases once they are scoped. The selected Bidder will work with VITL at all stages of these projects. The following breakdown of roles is anticipated.

Table 1 - R = Responsible; A = Accountable; C = Consulted; I = Informed

Role	VITL	Bidder
Project Scope, Communications and Organization	RA	RC
Project Work Breakdown, Milestones, and Timelines	RC	RA

Systems Architecture Procurement (SaaS, PaaS, IaaS)	RA	C
Systems Architecture Installation and Configuration	C	RA
Development and Integration	C	RA
Testing	RC	RA
Go Live Planning and Rollout	RA	RC
Ongoing Maintenance and Support	RA	RC
Ongoing Security Management and Vulnerability Remediation	RA	RC

Response Format

Responses are to be straightforward, clear, concise, and specific to the information requested. Proposals should be submitted in PDF format and be easily printable in 8.5 x 11 format. Send the proposal to VITL's point of contact. Paper proposals will not be accepted. All proposals must be complete. VITL reserves the right to eliminate any bidder whose proposal is incomplete in VITL's opinion. For submissions to be considered complete, vendors must provide the following information:

***Name and contact information**: for the person at your company who VITL should be in touch with regarding your response*

1. **General description of your company:**
2. **Services offered:** Please provide a description of your understanding of the scope of the engagement and the work that you are offering to provide. VITL, at its discretion, will consider the most optimal vendor(s) for the stated scope of work.
3. **Team members and roles:** List all personnel who would be assigned to this project and clearly indicate the role they would play. Include information about any other companies or freelancers you would partner with to complete this project. Let us know what resources VITL will need to devote to making this project successful.
4. **Offshore Resources:** Vendor must describe any potential offshore resource(s) necessary for the vendor's effort on this project. An attestation will be required affirming

   No data received, obtained, or generated by (company name) in connection with use of the system shall be processed, transmitted, stored, or transferred by any means outside the continental United States, except with the express written permission of VITL. Such data shall be restricted to prevent access from locations outside of the United States, such as through the use of security/access control mechanisms.
5. **VITL's role:** Briefly tell us how we can be a great client on this project.
6. **Proposed price:** Be sure to indicate which elements of the scope your proposed budget covers. We prefer that proposals give a fixed price for most elements.
7. **Proposed timeline for implementation:** Include key milestones along the way. The timeline should identify time commitments and milestones for VITL staff.
8. **References**: Please provide contact information for three individuals for whom you've completed a similar project in the last three years.
9. Appendix A, please complete the General Requirements Attachment
10. Appendix B, State of Vermont Attachments
11. Appendix C, VITL NDA (VITL will return a fully executed copy upon receipt)

Confidentiality and RFP Ownership

VITL reserves the right to recall this RFP in its entirety or in part. Vendors are granted permission to reproduce portions of this RFP in their responses. Vendors agree that they will not duplicate, distribute,

or otherwise disseminate or make available this document or the information contained in it without the express written consent of VITL's designated point of contact, identified above. Vendors must ensure that distribution or use of the RFP is limited within their organization and/or subcontractors on a need-to-know basis.

Vendors shall not include or reference this RFP in any publicity without prior written approval from VITL, which, if granted, shall be granted by the designated point of contact. Vendors must accept all of the foregoing terms and conditions without exception. All responses to the RFP will become the property of VITL and will not be returned.

Disclosure of Proposal Contents

Cost and price information provided in proposals will be held in confidence and will not be revealed or discussed with competitors, except to the extent required by law. All other material submitted becomes the property of VITL and may be returned only at VITL's option. Proposals submitted to VITL may be reviewed and evaluated by any person other than competing bidders at the discretion of VITL to assist VITL with evaluation of responses. VITL has the right to use any or all ideas presented in any response to the RFP. Where confidential or proprietary information is required, or should the vendor deem it necessary to submit such matter, the vendor must mark each page/section in large bold type (PROPRIETARY INFORMATION).

Contracting

VITL is subject to State of Vermont contracting requirements. As such, all VITL contracts must include standard State contract attachments known as Appendix Bx. Any vendor wishing to be considered must agree to these conditions.

Note that Appendix B contains specific insurance requirements which are excerpted below:

Insurance:

Before commencing work on this Agreement, the Party must provide certificates of insurance to show that the following minimum coverages are in effect. It is the responsibility of the Party to maintain current certificates of insurance on file with the State through the term of this Agreement. No warranty is made that the coverages and limits listed herein are adequate to cover and protect the interests of the Party for the Party's operations. These are solely minimums that have been established to protect the interests of the State.

Workers Compensation:

With respect to all operations performed, the Party shall carry workers' compensation insurance in accordance with the laws of the State of Vermont. Vermont will accept an out-of-state employer's workers' compensation coverage while operating in Vermont provided that the insurance carrier is licensed to write insurance in Vermont and an amendatory endorsement is added to the policy adding Vermont for coverage purposes. Otherwise, the party shall secure a Vermont workers' compensation policy, if necessary, to comply with Vermont law.

General Liability and Property Damage:

With respect to all operations performed, the Party shall carry general liability insurance having all major divisions of coverage including, but not limited to:

- Premises - Operations
- Products and Completed Operations Personal Injury Liability
- Contractual Liability
- The policy shall be on an occurrence form and limits shall not be less than:
- $1,000,000 Each Occurrence
- $2,000,000 General Aggregate
- $1,000,000 Products/Completed Operations Aggregate
- $1,000,000 Personal & Advertising Injury
- Automotive Liability: The Party shall carry automotive liability insurance covering all motor vehicles, including hired and non-owned coverage, used in connection with the Agreement. Limits of coverage shall not be less than $500,000 combined single limit. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, limits of coverage shall not be less than $1,000,000 combined single limit.

Additional Insured:

The General Liability and Property Damage coverages required for performance shall include the State of Vermont and its agencies, departments, officers, and employees as Additional Insureds. If performance involves construction, or the transport of persons or hazardous materials, then the required Automotive Liability coverage shall include the State of Vermont and its agencies, departments, officers, and employees as Additional Insureds. Coverage shall be primary and non-contributory with any other insurance and self-insurance.

Breach Notification Coverage/ Technology Professional Liability:

In addition to the insurance required in Sub-Attachment 2-C (Appendix C), before commencing work on and throughout the term of any Contract, the vendor agrees to procure and maintain (a) Technology Professional Liability insurance for any and all services performed, with minimum third-party coverage of $5,000,000 per claim, $5,000,000 aggregate. To the extent vendor has access to, processes, handles, collects, transmits, stores, or otherwise deals with State Data, Contractor shall maintain first party Breach Notification Coverage of not less than $10,000,000.

Before commencing work the vendor must provide certificates of insurance to show that the foregoing minimum coverages are in effect.

With respect to the first party Breach Notification Coverage, vendor shall name the State of Vermont and its officers and employees as additional insureds for liability arising out of this Contract as well as VITL.

Umbrella Liability:

Additionally, before commencing work, the vendor agrees to procure and maintain Umbrella Liability Insurance for any and all services performed, with minimum coverage of $4,000,000 per claim, $4,000,000 aggregate.

Vendor Attestation

In addition, any successful vendor must attest to the following:

- Vendor does not owe, is in good standing, or is in compliance with a plan for payment of any taxes due to the State of Vermont.

- Vendor is not on the State's disbarment list.
- Vendor (if an individual) does not owe, is in good standing, or is in compliance with a plan for payment of Child Support due to the State of Vermont.

The above provisions must be attested to annually. VITL will seek this attestation from the vendor on an annual basis.

Offshore Data Restriction

Vendor must also contractually commit to the following:

- No data received, obtained, or generated by VITL in connection with use of the system shall be processed, transmitted, stored, or transferred by any means outside the continental United States, except with the express written permission of VITL. Such data shall be restricted to prevent access from locations outside of the United States, such as through the use of security/access control mechanisms.

Termination for Lack of State Funding

VITL receives funding through its contract with the State of Vermont (the "State") on an annual basis. VITL may terminate the Contract upon ninety (90) days prior written notice to Contractor if, in VITL's sole determination, the State fails to provide sufficient funding for Contractor's Fees. Contractor shall be compensated for the services performed and costs incurred prior to the date of termination.

State of Vermont Contract Provisions

Please review the standard State of Vermont contract provisions and insurance requirements as described above and included in Appendix B and confirm that you are willing to accept these provisions in contracting and meet the insurance requirements as described.

Vendors should review these terms carefully prior to submission of a bid. Contact the VITL point of contact above with any questions or concerns regarding these State of Vermont contracting requirements.

Independent contractor

Please show that your company will be an independent contractor and not an employee as defined by the State of Vermont's Department of Labor. (The State's 'ABC' test for this is straightforward and the vendor should be able to quickly document that they meet the standards outlined here: https://labor.vermont.gov/document/who-employee-vs-independent-contractor.)

Additional Instructions and Information to Respondents

- All proposals submitted shall be binding for one hundred twenty (120) calendar days following the due date for the proposal.
- VITL reserves the right to award to the bidder(s) that presents the best value to VITL as determined solely by VITL in its absolute discretion.
- VITL is not responsible for any cost incurred by the bidder in either responding to this RFP or in participating in a meeting with VITL prior to award.
- VITL reserves the right to conduct discussions with bidders for the purpose of obtaining "best and final offers."
- VITL will make one or more awards for the requested services.

- There is no obligation on VITL's part to award any work packages (tasks) to an awardee.
- VITL reserves the right to reject any or all proposals in part or in full.
- VITL will evaluate its requirements for Access Management and API Security Management platforms to determine which awardee possesses the requisite expertise and ability and represents to VITL the best value for each individual task.
- VITL and the awardee will negotiate the work scope, schedule, and price for each task.

Summary Conditions

THIS IS A REQUEST FOR PROPOSAL (RFP) ONLY for Access Management and API Security Management platforms. The information provided in the RFP is subject to change and is not binding on VITL. VITL has not made a commitment to procure any of the items released in this RFP and the RFP should not be construed as a commitment or as authorization to incur costs for which reimbursement would be required or sought. All materials submitted become the property of VITL and be returned only at VITL's option. VITL reserves the right to reject any or all proposals in part or in full and to waive any technicalities or informalities as may best serve the interests of VITL.

Appendix A - General Requirements

The following table provides a breakdown of the critical elements that will inform VITL's selection. Please submit a brief response to each of these items in the column provided. Should your proposal be selected, you will be given the opportunity to further demonstrate your solution's capacity to meet each of these requirements with members of VITL's staff.

Description	Response
Introduction and Company Overview	
Describe your understanding of this engagement's scope and the work you offer to provide.	
Describe your firm's relevant healthcare and FHIR experience and/or any relevant projects you have completed.	
Tell us how we can be a great client, both during the implementation and ongoing through maintenance and support.	
Systems Architecture	
Describe the overall system architecture? Is the solution a complete SaaS offering, or based on 3rd party services and tools that VITL will procure?	
Describe how the solution will be readily extensible and scalable to meet future demands, such as the potential use cases defined in this RFP.	
How does the platform support high availability, minimal to no downtime for patching and maintenance, as well as geographic redundancy?	
Platform	
Demonstrate the key API Management capabilities of your platform, such as how to create and publish APIs or developer portal capabilities.	
Demonstrate the key identity provisioning methods of the platform, including how to manage user identities, certificates, tokens, etc. on the platform.	

Demonstrate the platforms authentication and authorization methods and support for MFA.	
Demonstrate the RBAC features of your system.	
Demonstrate the platforms support for single sign-on, federation, integration with other identity providers.	
Demonstrate how you manage, monitor and ensure the performance of APIs.	
Demonstrate the audit logging features of your system including events tracked during API usage.	
Demonstrate how the platform monitors responses and traffic to protect itself from being overloaded by too many requests	
Demonstrate how the platform detects and remediates real time threats, or malicious attacks.	
Describe the secure coding best practices, testing methodologies, or other security controls you employ to protect the security and privacy of the healthcare data behind these APIs.	
Project Overview	
Discuss your firm's approach and anticipated timeline for the installation and configuration of the baseline architecture.	
Describe your firm's approach to testing.	
Describe your firm's approach to go-live and transfer to operations.	
Ongoing Maintenance & Support	
Describe your firm's approach to design and implementation of projects like the potential use cases described in the RFP.	
What training do you recommend for VITL staff?	
Describe your firm's SLAs.	