Request for Information

State of Alaska
Department of Health and Social Services
Division of Public Health

Date Issued: October 16,2020

VacTrAK Immunization Information System

Introduction:

The Alaska Department of Health and Social Services, Division of Public Health, Section of Epidemiology is seeking responses from qualified parties capable and interested in providing and supporting an immunization Information System (IIS) for the State of Alaska. The Contractor will need to be able to support the data within the current Alaska IIS (VacTrAK), as well as maintain connections with healthcare providers to enter new data. All data entered into VacTrAK must be accessible via cloud-based computing and protected in accord with all IIS standards (both federal and state regulations). The IIS will consist of, at a minimum, a registry, inventory management system, and data exchange modules.

Background Information:

The current Alaska IIS (VacTrAK) is a web-based, confidential, population-based, computerized system that maintains immunization information for Alaskans of all ages. VacTrAK provides immunization resource management, and administration tools to track patients, entry of demographic and vaccination information and has the ability to generate reports. It is used to manage vaccine inventory and state supplied vaccine orders. VacTrAK helps public health agencies and health care providers to make informed decisions to improve the health of individuals and the entire community.

Scientific Technologies Corporation (STC) has been the IIS vendor since 2007.

The Alaska IIS contains (data as of 9/15/20):

- 1,495,885 patients in the registry (NOTE: This number is larger than Alaska's population because health care providers do not always inactivate patients who move out-of-state. This is a national immunization information system problem.)
- 13,703,852 total vaccinations
- 318 health care organizations/facilities use the system (including pharmacies like Costco, Walmart, etc.)
- 2,973 active users

VacTrAK users currently utilize all of the following modules:

- IWeb: Vaccine Registry with consolidated patient records, deduplication, clinical decision support tools to ACIP forecast recommendations, coverage rate reports, reminder and recall functions for notification of patients due for vaccine.
- VOMS (Vaccine Ordering and Management System): Allows for streamlined management of vaccine supplies (both public and private) for both manual entry and EHR connected providers, compliant with CDC's Vaccine Tracking System (VTrckS), and provides a convenient way to handle orders directly from within the IIS.

- PHC-Hub: Interoperability supports high-quality HL7 messaging and allows for bidirectional transport of data in a clean and easy to administer format following multiple transport methods endorsed by CDC, including the Simple Object Access Protocol (SOAP) standard Interface and Web Services Definition Language (WSDL).
- iQ: A state-of-the-art intelligence dashboard that was developed collaboratively and designed to identify, inform and impact the quality of data submitted electronically to the IIS.
- Perinatal Hepatitis B Module: A case management tool used to identify and track Hepatitis B positive pregnant women to ensure that their infants receive the necessary post-exposure follow-up to protect them from Hepatitis B. The module helps the State monitor and support Hep B positive pregnant women before birth and their infants' post-birth through vaccine queries of the IIS and notifications regarding vaccine needs that are identified.
- Mass Immunizations: A field application to quickly conduct entry of demographic and vaccination information gathered in mass immunization situations. The interface is optimized for speedy entry of an appropriately limited set of data elements. Reports, reminder/recall, and other assessments are conducted from the central registry once loaded with the field data.
- STC|U: A learning management platform that enables immunization programs to create a course catalog, course reports and quizzes, as well track participant's completion status and scores through a course gradebook.
- SMaRT AFIX Hosting: Coverage rates and missed opportunities information are presented in easily understood graphic displays. Patient lists to support patient management, missed opportunities and invalid dose reporting. Also available to providers for self-assessment. SMaRT AFIX simplifies the process of reporting the AFIX assessment results to the CDC.

Scope of Work:

The Contractor shall:

- Ensure that Alaska's IIS, meets all applicable regulatory State and federal requirements.
- Provide on a timely basis, price quotes and system modifications documentation, as needed to assist the State in obtaining state or federal funding.
- Provide the State with all new patch/fix releases and/or version upgrades to software applications at no cost to the State.
- Provide queries to perform data extractions and assist in data analysis.

Deliverables:

VacTrAK Software Maintenance

The following maintenance deliverables/services will include:

- Regular releases to include new functionality and bug fixes. The major release cycle must be supported by a patch cycle to be approved by the Immunization Program IIS Manager.
- IIS Functional Standards will be maintained, including the performance measures and quantitative targets set by the Centers for Disease Control and Prevention (CDC), as measured by the CDC IIS Annual Report (IISAR). Version 4.1 at the time of contract.
- Support the completion of the CDC IIS Annual Report. Develop and implement IIS scripts annually, according to specifications provided by CDC and provide production data reports at least 30 days prior to the due date.
- National standards for electronic data exchange will be maintained, including the current specifications laid out in the CDC HL7 Implementation Guide (2.5.1 version 1.5 at time of contract) and inclusive of backward compatibility.

- Implement feedback from the American Immunization Registry Association (AIRA)-sponsored IIS Measurement and Improvement (M&I) Initiative Aggregate Analysis Reporting Tool (AART) for conformance with current CDC IIS Interoperability Standards and IIS community compatibility. Validation measures to include HL7 Transport Assessment, Submission and Acknowledgement, and Query and Response.
- All new vaccines and Advisory Committee on Immunization Practices (ACIP) schedule changes will be implemented under the maintenance agreement and will be made available to the Alaska IIS within 30 days of the Morbidity and Mortality Weekly Report (MMWR) publication release announcing the recommended vaccine schedule to providers.
- Maintain ACIP forecast and improve consistency and quality of evaluation and forecasting using CDC Clinical Decision Support for Immunization (CDSi) published logic specification guidance and supporting data. Version 4.1 at the time of this contract.
- Help Desk Services:
    - Hours of operation: Monday – Friday, 8AM-5PM Alaska Standard Time.
    - Help Desk staff via calls and emails
    - Online Service Desk, help desk software accessible to State users
    - Monthly Help Desk status calls
    - Maintain a Service Level Agreement and maintain defined response time and process for critical and non-critical issues
- Documentation:
    - Release/patch notes
    - Updated documentation with each release
    - New documents created based on client needs or requests
    - Documentation portal accessible by all clients
- Documentation of weekly maintenance for cloud hosted environments and quarterly review of regular maintenance schedule for accuracy and updates.
- Log all updates and/or changes applied to VacTrAK with each application patch/fix releases or version upgrades and provide to the systems managers within 10 business days of the system changes.
- Downtime notification process and review of root cause.
- Provide a Consortium of States using vendor's IIS Software Products
    - Enhancement leveraging between consortium members
    - Facilitation of leveraged effort opportunities
    - Monthly conference calls for information exchange and decision making
    - Annual User Group Meeting

Cloud Hosting Services for VacTrAK Applications

The current IIS vendor provides cloud hosting services through Amazon Web Services (AWS) for the entire product suite that is utilized by the Immunization Program. The current vendor designed a Health Insurance Portability and Accountability Act (HIPAA)-compliant architecture based in the United States and employs multiple servers where necessary to ensure redundancy, failover and backups.

The current vendor's solution meets relevant HIPAA guidelines, in particular the Privacy Rule and Security Rule. The vendor maintains a Business Associate Agreement with Amazon and is the preferred vendor for hosting due to Amazon's proven security and reliability. Security procedures include event logging, vulnerability management, virus protection. The current vendor practices a policy of continuous improvement regarding security and regularly reviews all aspects of security to seek out issues and opportunities for improvement. The Contractor will need to offer a product that can adhere to these guidelines, provide the same protections, and provide similar quality guarantees. Additionally, the Contractor will need to provide the same environments, and modules within those environments, listed below.

The Alaska IIS requires the 3 environments included under this contract:

1. VacTrAK Production
2. VacTrAK Test/Staging
3. UAT (User Acceptance Testing) – an environment with no Alaska patient data

Modules included:

- **IWeb:** Vaccine Registry with consolidated patient records, deduplication, clinical decision support tools to ACIP forecast recommendations, coverage rate reports, reminder and recall functions for notification of patients due for vaccine.
- **VOMS** (Vaccine Ordering and Management System)**:** Allows for streamlined management of vaccine supplies (both public and private) for both manual entry and EHR connected providers, compliant with CDC's Vaccine Tracking System (VTrckS), and provides a convenient way to handle orders directly from within the IIS.
- **PHC-Hub:** Interoperability supports high-quality HL7 messaging and allows for bidirectional transport of data in a clean and easy to administer format following multiple transport methods endorsed by CDC, including the Simple Object Access Protocol (SOAP) standard Interface and Web Services Definition Language (WSDL).
- **iQ:** A state-of-the-art intelligence dashboard that was developed collaboratively and designed to identify, inform, and impact the quality of data submitted electronically to the IIS.
- **Perinatal Hepatitis B Module:** A case management tool used to identify and track Hepatitis B positive pregnant women to ensure that their infants receive the necessary post-exposure follow-up to protect them from Hepatitis B. The module helps States monitor and support Hep B positive pregnant women before birth and their infants' post-birth through vaccine queries of the IIS and notifications regarding vaccine needs that are identified.
- **Mass Immunizations:** A field application to quickly conduct entry of demographic and vaccination information gathered in mass immunization situations. The interface is optimized for speedy entry of an appropriately limited set of data elements. Reports, reminder/recall, and other assessments are conducted from the central registry once loaded with the field data.
- **Learning Management System:** A learning management platform that enables immunization programs to create a course catalog, course reports and quizzes, as well track participant's completion status and scores through a course gradebook.
- **SMaRT AFIX Hosting:** Currently, the CDC supports the ongoing maintenance of the application for participating awardees (subject to ongoing funding and being accepted by CDC into the maintenance contract), but not the hosting costs. Therefore, STC includes the hosting of SMaRT AFIX within the STC|ONE Public Health IIS Essentials Package. STC developed the SMaRT AFIX with the CDC and 17 other IIS programs through collaboration to make the IQIP vaccination coverage assessments easy and actionable for providers.

Refresh TEST VacTrAK environment with copy of production data at least once annually; implementation date to be approved by Immunization Program Manager.

DHSS IT Standards and Security Requirements

The vendor must comply with the security requirements outlined in the DHSS Security Plan for VacTrAK, including Appendices, G, H, and I.

Some requirements from the DHSS Security Plan include:

1. **Security** (Hosting infrastructure for the entire Immunization Information System)**:** As DHSS (Covered Entity) IT does not have control of off-site hosted environments, any and all security mechanisms for

hosted applications and data outside the State network falls to the responsibility of the vendor (Business Associate). This includes encrypting and securing any confidential data and adopting the latest security measures available to prevent unauthorized access. As part of the security controls, this includes application/operating system/firmware patching, minimizing administrative controls, and providing a detailed Security Plan, that includes NIST Control responses, to our Department Security Office (DSO) for review and approval. The security plan must be approved by the DSO before systems or applications are authorized for production. The vendor assumes the responsibility for any and all authentication and account creations or modifications.

2. **BAA:** The signed and executed DHSS Business Associate Agreement must remain in effect for the duration of this contract.

3. **Data Ownership:**
   a. All files containing any confidential or legally protected information are the sole and exclusive property of the State. The contractor agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from the State. Contractor agrees to abide by all federal and State confidentiality requirements.
   b. The Department of DHSS is considered a covered entity in regard to HIPAA which governs security requirements for electronic protected health information (ePHI) and HIPAA. DHSS owns the data and can demand it at any time. The vendor will expeditiously provide it to DHSS upon request.

4. **Network code scans:** Systems and applications hosted off-site must have FISMA (NIST 800-37) authenticated network vulnerability scans performed at least once every 30 days, with the results securely provided to the Department Security Office (DSO) and the Division Data Owner. The scanning tool and configuration/settings must be documented and presented to the DSO for review and approval before use. DSO approval is required and cannot be changed without DSO approval. Findings of Medium Risk and above must be remediated in the following timeframes. The vendor will notify the DHSS Chief Security Officer (CSO) when issues are not addressed within the following criticality dependent time periods.
   - Very High: 5 business days
   - High: 10 business days
   - Medium: 20 business days

5. **Static Code Scans:** Applications hosted off-site must have an automated static code scan using Veracode, with scans run before code changes are posted, and at least once every 90 days, with the results provided to the Department Security Office and the Division Data Owner. Comparable alternatives to Veracode will be considered and must be approved by the Department Security office.

   For new software modules, an automated static code scan must be performed using the DHSS licensed version of Veracode and the vendor will notify the DHSS Chief Security Officer (CSO) when issues are not addressed within the following critically dependent time periods for new software modules:
   - Very High: 90 days
   - High: 120 days
   - Medium: 180 days

6. **Web-Application Firewall:** Applications and servers hosted off-site must be protected by a web-application firewall (WAF), configured to prevent hostile behavior. The WAF will be subject to change management practices, will be documented in the security plan, and will have active support with a maintenance contract.

7. **Security Patching:** The process that will be used to apply, test and validate the appropriate patches and updates must be defined.

8. **Logging and Auditing:** For off-site hosting, there must be a logging and auditing solution. All systems are required to be configured to generate logs when a particular user (standard or privileged): creates, reads, updates, and/or deletes data at a particular time. For example, a log meeting this requirement may state: "User jasmith viewed patient record A32867 at 9:37:01 AM AKST." The application must be readily capable of generating logging and auditing in a concise summary that can be easily subject to research by indexing. The industry standard solution the offeror chooses to implement must be described, and must provide responsible DHSS entities (DSO, Data Owner) secure remote access to perform oversight related tasks. The package that is produced by the application must able to be inclusive of all the data for who is accessing, reading, and writing the data.

9. **Operating System:**
    a. Operating System Patching- Department, State, and Federal security standards are enforced through a number of security controls which require coordination with the Department Security Office (DSO) and the DHSS Security Plan template to document the approach, methodology, roles and responsibilities, and processes and procedures with respect to the Technical Contractor's tasks.
    b. All sensitive, confidential, and/or restricted data is encrypted in-transit and at-rest using a NIST FIPS 140-2 certified product.
    c. Sensitive and/or confidential data includes Electronic Protected Health Information (ePHI), as defined in the Federal Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) as defined by the US Privacy Act and Personal Information (PI), as defined in the State of Alaska Personal Information Protection Act (APIPA, AS 45.48).
    d. Security controls are audited for the DHSS Risk Assessment regardless of whether an application/solution is hosted on premise or elsewhere. The Department's current IT security compliance standards are specified in Appendix H (the DHSS Security Plan) including the requirement to document the controls specified and to have that plan be approved by the DHSS Security Office
    e. Vendor must address how frequently they roll out releases and method of notification.

10. **Desktop Access Requirements:**
    a. The vendor must delineate the desktop access requirements by the hosted application. Note: Applications delivered via Web software should be browser and device independent. State staff does not have administrative rights for their machines. If there are specific active X, or other plug-in's, they must be kept patched and must be identified.
    b. Software should not be dependent on a specific version of Microsoft Office Suite. For example, DHSS is currently at Office 365 and the entire organization is upgraded at one time for Microsoft upgrades.

11. **Browser Settings:**
    a. The vendor must address what browsers are optimal for software solution (and version of browser), as well as those browsers in which software solution performs poorly.
    b. The vendor must provide what browser settings and add-ins will be needed for the solution and define what the process is for ensuring your application supports the latest browser versions as they are updated and how they will notify the user.
    c. Software should not be dependent on a specific brand or version of web browser. Software should support the current versions of Internet Explorer, Edge, FireFox, Chrome, and Safari.

12. **Disaster Recovery:** The vendor will provide a disaster recovery plan as an addendum to the DHSS Security Plan and will update the disaster recovery plan as systems or plans are updated.

13. **Test Environment and Migration to Production:** The vendor will define the change management and communication process between State of Alaska Immunization Program staff, the DSO and STC for updating the test environment and production environment.
14. **Vendor Help Desk Support:** Vendor Helpdesk response interaction and established procedures must be defined. Application maintenance and enhancements procedures must be defined for current functions.
15. **Data Archiving and Record Retention:** The Vendor will be required to comply with the Department of Health & Social Service's policies and procedures for record retention and disposal of sensitive information. Audit logs must be retained and remain available for a minimum of six years, and changes to patient data files are permanent.
16. **Termination of Services:** Provide a successful transition of VacTrAK over to the State or its designee at the expiration or termination of this Agreement. DHSS will be provided a full copy of VacTrAK Production Systems data and a perpetual license to continue use of applications if STC goes out of business or otherwise terminates services. STC will provide immediate written notice to DHSS if they suspect a reasonable chance that STC be out of business within 90 days.

Budget:

For these Services, the State Contracting Agency shall pay the Contractor in one lump sum at the start of the contract. Each additional year will be evaluated and revised, if necessary, during the annual renewal period.

The Contractor should be prepared to meet all the deliverables listed above for $758,000. The Contractor will be required to provide an itemized price sheet of each module provided.

Minimum Qualifications:

The Contractor must:

- Have 10 or more years in providing IIS software services, with at least 3 of those years providing a cloud-managed IIS service
- Offer a product that maintains the IIS Functional Standards, is HIPAA-compliant, meets DHSS IT standards, and provides built-in analytics
- Offer a product that can utilize a bidirectional HL7 connection between VacTrAK and all immunization providers in the State of Alaska.
- Offer a consortium of 3 or more states that use its IIS software services
- Provide a service that allows patients direct access to their immunization records
- Provide and support a system that meets all IIS Program Requirements and must be 100% complaint with CDC/NCIRD IIS Functional Standards v4.0.

Response Information:

Interested proposers must submit an electronic response, 3 pages maximum, with the following information:

- Proposer Name (business name or individual)
- Authorized signer
- Mailing & physical address
- Phone number
- Email address
- A description of how the applicant meets or exceeds the experience requirements.
- Information about where to obtain a product demo
- A statement confirming that the firm anticipates the project deliverables, as described above, are reasonably within the estimated budget provided. Or, if not, why not?

- A brief summary of any concerns regarding the project as described. What potential obstacles should be anticipated?

Submit an electronic response no later than 4:00 pm, Alaska Prevailing Time, October 26, 2020 to hss.procurement.proposal@alaska.gov, Attention: Kellie Julian.

Kellie Julian, Procurement Officer
(907) 465-5293
kellie.julian@alaska.gov

BIDDERS/OFFERORS WITH DISABILITIES: The State of Alaska complies with Title II of the Americans with Disabilities Act of 1990. Individuals with disabilities who may need auxiliary aids, services, and/or special modifications to submit a Letter of Interest should contact the Procurement Specialist named above, no later than October 21, 2020.

Important Notice:

This RFI does not extend any rights to prospective vendors or obligate the state to conduct a solicitation or purchase any goods or services. Nor will the State be financially responsible for any costs associated with the preparation of any response for the requested information. This RFI is issued for the sole purpose of obtaining information as described in this notice. However, the information obtained from this request may be used to prepare a purchase, contract, or solicitation in the future.