Reference A
Information Technology Requirements

State of Alaska
Department of Health

TABLE OF CONTENTS

1 Purpose of IT Requirements 2

1.1 IT Requirements Intent and Approach 2

2 Technical Qualifications Response 4

2.1 Minimum Qualifications 4

2.2 Understanding of the Technical Aspects of the Project 4

3 State of Alaska DOH Technology Services, Standards, and IT Road Map 5

3.1 DOH Information Technology Services Staffing Support 5

3.2 Engagement and Service Delivery Management Services and Standards 6

3.3 Project Portfolio Management Services and Standards 7

3.4 Asset Management Services and Standards 8

3.5 Systems Integration and DDI Services and Standards 10

3.6 Systems Operations and Administration Services and Standards 14

3.7 Information Security Compliance and Privacy Services and Standards 16

3.8 Enterprise Desktop and Mobility Services and Standards 20

3.9 DOH Hosting and Datacenter Services and Standards 22

3.10 DOH Wide Area Network, Telecommunications, and Perimeter Security Services and Standards 23

3.11 Accessibility 24

3.12 State of Alaska DOH MITA Standards and Department IT Technology Standards 25

1 Purpose of IT Requirements

The State of Alaska Department of Health (DOH) is engaged in a Cloud First initiative strongly favoring SaaS solutions. We have embraced an Information Technology (IT) Roadmap for shared services using our Enterprise Service Bus (ESB), and Master Client Index (MCI).

The response to this request must address if, and how, the proposed product solution will integrate into this environment, where appropriate.

1.1 IT Requirements Intent and Approach

DOH Information Technology Services (ITS) values our partner relationships with external vendors, contractors, and grantees. DOH ITS is focused on providing the best value to our customers by supporting IT procurements from the RFP solicitation process, through project initiation, planning, execution, and closing.

At a high-level, these IT requirements support the proposal solicitation by meeting two goals:

1. The requirements help the Offeror understand our service delivery approach. They give Offerors the opportunity to shape their proposals to best fit the team of program staff, ITS staff, and Offeror staff that will work together to deliver the solution.
2. The requirements identify specific requirements and statements that Offerors must address to be classified as responsive.

These IT requirements are structured into services and standards sections, corresponding to a service line within DOH ITS. For example, the solicitation-relevant requirements for end-user desktop configurations are in the “Enterprise Desktop Services and Standards” section.

As part of our Cloud First initiative, DOH IT is seeking proposals for solutions which are vendor hosted and vendor managed, rather than provided locally or hosted within the department’s network.

However, we recognize that solutions are available in many forms. Offerors may consider proposing one or more of the following options:

- DOH hosted and managed solution components;
- 3rd party hosted, DOH managed solution components;
- Software as a Service (SaaS)
- Anything as a Service (XaaS);
- Hybrid/Combination of above.

DOH recognizes that SaaS and XaaS delivery models afford some additional value to our department. It offers the opportunity to leverage the business value of the solutions without bearing the costs and risks of having to maintain development and operational infrastructure. This value is achieved when the SaaS/XaaS vendor carries the burden of managing technical operations and ongoing development/maintenance, while collaborating with their clients to meet and maintain the functional requirements and integrity of the solution.

Offerors should read each section carefully to understand how DOH ITS applies a particular service-line to procured services and what specific requirements, questions, and statements must be answered. Please be aware that the State of Alaska requires all resources utilized as a part of the RFP response, system development, and implementation to be US based or DOH approved resources. This includes hosted services, vendor personnel, vendor contracted services, and personnel and vendor contracted consulting services.

2 Technical Qualifications Response

2.1 Minimum Qualifications

Offerors must complete **Required Vendor Response - DOH IT Requirements**, which correspond to the requirements described in Section 3 of this document and return it as part of their proposal. A failure to complete and return this IT Reference will result in a proposal being deemed non-responsive.

2.2 Understanding of the Technical Aspects of the Project

In the body of their proposal, Offerors must provide comprehensive narrative statements that illustrate their understanding of the technical requirements and must respond to all applicable sections, or respond why a section is not applicable.

A failure to demonstrate how the solution being proposed addresses the Technical Requirements outlined may result in the proposal deemed non-responsive and rejected.

3 State of Alaska DOH Technology Services, Standards, and IT Road Map

Information technology services for DOH agencies are provided by DOH Division of Finance and Management Services Information Technology Services (ITS). DOH ITS provides the following functions: maintenance of the DOH Data Centers in Juneau and Anchorage; project execution support; operational support; and integration assistance for systems hosted on site. We also manage some IT services hosted and operated out of the State of Alaska Office of Information Technology (SOA-OIT) data centers (separate from our datacenters), and services out of Microsoft's Azure Government Community Cloud.

This section describes many of the services offered in detail and highlights elements of our IT Environment we think you need to know to work with us.

3.1 DOH Information Technology Services Staffing Support

Regardless of whether the Offeror proposes a totally outsourced, partially outsourced, or hosted on DOH Premise solution, expectations for support must be clearly defined.

DOH ITS staffing support hours are:

- Customer & Application Support hours are M-F, 8:00am to 5:00PM Alaska Time
- Network Support hours are M-F, 7:00AM to 5:00PM Alaska Time

Support from DOH ITS required outside of those hours, including evening and weekend batch job support, must be defined and documented. This must include the duties and expectations for DOH ITS staff. All hours of operation **must be expressed in Alaska Time.**

3.1.1 Requirement – Production Operations Phases

The Offeror must:

- Define and document a schedule of hours they plan to operate, including the time zone(s) they plan to operate from;
- Identify hours their staff will work outside of the DOH ITS standard hours, defined in this section;
- Identify the daily schedule of hours during which they expect DOH ITS and DOH Program staff to support the activities under the execution of the proposal;
  - The schedule will include and differentiate hours for end-user access and hours for technical support, including any offline batch or after-hours system maintenance activities.
- Commit to deliver a plan that includes Offeror and DOH agreed upon daily scheduled hours.
  - The plan must also include the schedule of Offeror and State of Alaska observed holidays.
  - SOA Holidays can be found at: https://doa.alaska.gov/calendar/
- ***If solution is to be DOH managed in the Production and Operations*** phase, additional requirements are:
  - The Offeror's proposal must include a solution that requires no regular after-hours system support
  - If the Offeror's proposed solution requires after-hours system support, the Offeror must reach formal agreement via:
    - An accepted Operations Support Model deliverable;
    - The OIT Department Technology Officer for DOH and DOH Assistant Commissioner approval.
    - This agreement must be reached at least 6 months prior to commencement of proposed training activities that precede DOH assuming operational responsibilities for the solution.

3.2 Engagement and Service Delivery Management Services and Standards

Engagement and Service Delivery Management Services includes the activities DOH ITS performs to engage with our DOH Program staff and manage delivery of all IT services. This includes defining the organization's requirements, assisting with DOH IT Governance alignment, change request processes, and applying and managing the correct DOH ITS service-lines for specific DOH ITS initiatives and procurements.

3.2.1 Contract Negotiations ITS Review and Approval

DOH ITS participates directly on the contract negotiations team to review and approve all IT related contract elements further specified in the final contract.

3.2.1.1 Requirement – IT Contract Review

The Offeror must be prepared to work with DOH ITS, Procurement, and Program staff to review and approve all IT related contract elements.

3.2.2 Project Kickoff Service Alignment Conference

As part of project kickoff activities, DOH ITS and Program representatives will meet with the Offeror's execution team to agree upon the necessary DOH ITS service lines required to support the execution of the procurement. This activity will be based on a review of the scope and schedule defined in the solicitation, the proposal, and the final contract.

The outcome will be a list of DOH ITS service lines supporting execution of the procurement and a list of any gaps identified by the Service Alignment Conference team. Gaps identified may include services or products DOH ITS does not support, DOH ITS staffing resource constraints, or other gaps.

3.2.2.1 Requirement – DOH ITS Service Alignment Conference

The Offeror must include project activities to reach agreement with DOH ITS and DOH Program staff on DOH ITS support service lines and identify any gaps. All gaps identified must include a plan of action to address and resolve the gaps.

3.2.3 DOH Service Line Engagement and Planning

Different procurements require customized support activities to succeed within scope, schedule, and resource constraints. To ensure the best outcome, the DOH ITS service lines identified to support the procurement will work with DOH Program staff and Offeror staff to roadmap the service line engagement schedule, review the gaps identified in the service alignment conference, and detail the action plans to address those gaps.

3.2.3.1 Requirement – DOH IT Service Line Engagement and Planning Workshops

The Offeror must include project activities to reach agreement with DOH ITS and Program staff on the service line engagements identified in the Service Alignment Conference deliverables. These activities must roadmap the schedule of service line engagements, identify the service line team members, review the gaps previously identified, and detail the action plans to address those gaps.

3.2.4 DOH Service Line Management Processes and Tools

DOH ITS service line staff will use their standard, defined processes and management tools to document and manage their work (See Sections 2.1 and 2.2 of Information Technology Standards Reference D).

For cost and operational efficiency, DOH ITS prefers that the Offeror align their processes and tools with those of DOH ITS. The Offeror may propose leveraging the DOH processes and tools in their proposal.

3.2.4.1 Requirement – Service Line Management Processes and Tools Alignment

DOH prefers the Offeror be prepared to work with DOH ITS service line management processes and tools. For each DOH IT service line supporting the project, the Offeror must review the applicable processes and tools with DOH ITS and DOH Program staff to align processes and tools of the project with those used by DOH ITS.

If the Offeror and DOH Program staff determine a benefit to using alternate tools, the Offeror must accept the cost of any duplication of effort required of either the Offeror's staff or DOH Program staff to maintain and synchronize requirements, documentation, service requests or other artifacts applicable to the DOH ITS service line.

Whichever tools are selected, the Offeror must document agreed upon decisions made with DOH ITS and DOH Program staff.

3.2.5 DOH Managed Off-site Hosting Scenarios

All DOH Engagement and Service Delivery Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.2.5.1 Requirement

The Offeror must understand and acknowledge 3.2.5.
The Offeror must identify any elements of your proposed solution that will be hosted outside of DOH datacenters.
The Offeror must identify the geographic location of each of those elements.

3.2.6 Software as a Service (SaaS) and Anything as Service (XaaS) Scenarios

All DOH Engagement and Service Delivery Management Services and Standards apply to SaaS/XaaS scenarios.

3.2.6.1 Requirement

The Offeror must understand and acknowledge that all DOH Engagement and Service Delivery Management Services and Standards apply to SaaS and XaaS scenarios.

Identify any elements of your proposed solution that will be fulfilled via Software-as-a-Service delivery models.

3.3 Project Portfolio Management Services and Standards

See IT Reference B—DOH Project Management Requirements.

3.3.1 DOH Managed Off-site Hosting Scenarios

All DOH Project Portfolio Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.3.1.1 Requirement

The Offeror must understand and acknowledge 3.3.1.

3.3.2 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

All DOH Project Portfolio Management Services and Standards apply to SaaS/XaaS scenarios.

3.3.2.1 Requirement

The Offeror must understand and acknowledge 3.3.2.

3.4 Asset Management Services and Standards

Asset Management Services include the activities DOH ITS performs to manage software licensing and other software and information assets. DOH considers all data, software source code, configuration files, binaries, licenses, and configured systems as "assets". DOH Policies and Standard Operating Procedures require that stewards, responsible for creating and maintaining assets, properly manage these assets. This means asset stewards should apply proper inventory and version control practices to ensure individual assets are identified and version consistent artifact sets can be recreated to support disaster recovery, testing, audit, and other scenarios.

3.4.1 Artifact Version Management

DOH ITS operates a document and code management repository that supports version control (see Information Technology Standards Reference D). The Offeror must transfer ownership of all project artifacts to DOH as part of the scope of work, including the effort to convert/migrate the artifacts into the DOH artifact version management repository. To reduce project overhead and transition costs, the Offeror is encouraged to use the DOH artifact version management repository during project execution.

3.4.1.1 Requirement

Requirements, design documents, source code, configuration files, and binaries that are versioned over time must be managed in one or more version control repositories such that any released version of these artifacts can be retrieved later to rebuild the information system or application. Platforms that support configuration changes via a graphical user interface must support an extract of the changes made that can be loaded into the version control repository and release-managed in an equivalent manner to source code.

3.4.2 Licensing Agreement

3.4.2.1 Requirement

The license shall include, but not be limited to:

- All supporting programs in the most current version;
- All scripts, programs, transaction management or database synchronization software, and other system instructions for operating the system in the most current version;
- All data files in the most current version;
- User and operational manuals and other documentation;
- System and program documentation describing the most current version of the system,
- The most current versions of source and object code;
- Training programs for the State and other designated State staff, their agents, or designated representatives, in the operation and maintenance of the system;
- All performance-enhancing operational plans and products, exclusive of equipment; and
- All specialized or specially modified operating system software and specially developed programs, including utilities, software, and documentation used in the operation of the system.

Ongoing upgrades of the application software and supporting 3rd party programs must be provided through the end of the contract.

Any other specialized software to be integrated into the system, and not covered under a public domain license, must be identified as to its commercial source and the cost must be identified in the Cost proposal. DOH may, at its option, purchase commercially available software components itself.

The contractor must convey to DOH, upon request and without limitation, copies of all interim work products, system documentation, operating instructions, procedures, data processing source code, and executable programs that are part of the system, whether they are developed by the employees of the contractor or any subcontractor as part of this contract or transferred from another public domain system or contract.
The provision of this section related to ownership/support for the product must be incorporated into any subcontract that relates to the development, operation, or maintenance of any component part of the system.

3.4.3 Software Procurement Assurance – Guaranteed Access to Software

3.4.3.1 Requirement

DOH shall have full and complete access to all source code, documentation, utilities, software tools, and other similar items used to develop/install the proposed solution or may be useful in maintaining or enhancing the equipment and solution after it is operating in a production environment.

DOH executive leadership may choose to waive the above requirement upon written request explaining your unique business need. SaaS/XaaS solutions may also request waivers for these requirements (see 3.4.7).

In such cases any of the above-mentioned items not turned over to DOH upon completion of the installation, the Offeror must provide a written guarantee to DOH of uninterrupted future access to, and license to use, those items. The guarantee must be binding on all agents, successors, and assignees of the contractor and subcontractor. State access to source code may be protected by use of a third-party escrow account.

If an escrow account is used, the terms must include at a minimum:

- Update of the source code in escrow as often as required for the source code to reflect the current version of each application of the software licensed by DOH.
- DOH has the right to view or access the source code to:
  - Verify the source code's completeness and readability of the media.
  - Obtain a copy of the source code in the event of a filing of Bankruptcy where the Offeror is no longer able to provide acceptable service.
  - Obtain a copy of the source code if the Offeror ceases to do business completely, or to do business in the line of business marketplace the system supports.

DOH reserves the right to consult legal counsel as to the sufficiency of the licensing agreement and guarantee of access put forth by the Offeror.

3.4.4 Software Procurement Assurance – Federal Rights

3.4.4.1 Requirement

If a federal grant was used for this solution, the federal government reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for federal government purposes, the copyright in any work developed under a grant, sub-grant.

3.4.5 Data Ownership

3.4.5.1 Requirement – Data Ownership

DOH shall have unlimited rights to use, disclose or duplicate, for any purpose whatsoever, all information and data developed, derived, documented, installed, improved, or furnished by the Offeror under this contract.

All files containing any DOH information are the sole and exclusive property of DOH. The Offeror agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from DOH. Offeror agrees to abide by all federal and state confidentiality requirements.
In addition, the Offeror agrees to provide to DOH, at the end or at any time during the contractual period, the data managed by the solution, in whole or in part, in a format agreed upon by both parties.

3.4.6 DOH Managed Off-site Hosting Scenarios

All DOH Asset Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.4.6.1 Requirement

The Offeror must understand and acknowledge 3.4.6.

3.4.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH ITS expects that by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Asset Management Services and Standards.

3.4.7.1 Requirement

If proposing SaaS/XaaS components for all or part of the solution, the Offeror's proposal must comply with all Asset Management Services and Standards requirements.

The Offeror may propose leveraging variations or exceptions under this subsection, *Software as a Service Scenarios (SaaS) and Anything as a Service (XaaS)*. If the Offeror wishes to leverage variations or exceptions, these must be defined. If exceptions are to be requested please clearly outline

- Which requirement you are seeking an exception for
- What alternative measure you are offering in its place
- How the department's interests will be protected, even in the event the Offeror goes out of business or files for bankruptcy

3.4.7.2 Requirement – Data Stewardship

The Offeror will maintain Alaska's data in the solution for the life of the contract. The Offeror must explain how data will be archived for the solution. Turnover requirements will be negotiated between DOH and the Offeror to ensure that all DOH data will be returned to DOH in a cooperative manner at the close of the contract or the decommissioning of the solution. DOH data may include; deliverables, reports, configuration details, business requirement documents, test plans, scripts, and results.

3.4.7.3 Requirement – Geographic Location Identification

The Offeror must identify the geographic location of any non-DOH hosted external information systems that receive, process, store, or transmit proposed solution data.

3.5 Systems Integration and DDI Services and Standards

DOH ITS provides a full range of Systems Integration and Design, Development, and Implementation (DDI) Services. These services follow DOH standards to ensure maximum leverage of staff and other resources and ensure scalability. DOH expects the Offeror to understand and align their proposal and activities with DOH Systems Integration and DDI Services and standards.

The most noted points of integrations include:

- Our department's information exchange architecture;
- Master data management;

- Integrated Resource Information System (IRIS) and Alaska Data Enterprise Reporting (ALDER) integration;
- Authentication and Single Sign-On.

Maintaining alignment will be an ongoing activity during the project. However, the Offeror must demonstrate how they anticipate reaching alignment within their proposal.

3.5.1 Information Exchange Architecture

To simplify the effort and reduce costs of DOH systems implementation and long-term operations, DOH has implemented an Enterprise Service Bus (ESB) that supports system integration and information exchange. Additionally, DOH has partnered to create an Alaska statewide Health Information Exchange (HIE). Together, the ESB and the HIE can substantially reduce the operational complexity of moving data between systems hosted on-premise or in the cloud.

3.5.1.1 Requirement

Data exchange interfaces must leverage the DOH Enterprise Service Bus and/or the statewide HIE, where applicable.

The Offerer must describe

- What interfaces and data exchange processes do you anticipate implementing with the HIE?
    - If you do anticipate implementing these processes, please describe how the proposed solution would transfer data to and from the HIE, as applicable.
- What interfaces, data exchange processes and services do you anticipate implementing via the DOH Enterprise Service Bus (ESB)?
    - If you do anticipate implementing these processes, please describe how the solution would transfer data using this method?
- Your architectural approach to transferring data sets to/from your system. Include both single-record/case and batch transfer scenarios.

3.5.2 Master Data Management

DOH has implemented master data management services for client/consumer/person demographic records via the DOH Master Client Index (MCI). The MCI connects client demographic records across applications and systems.

Solutions that create, read, or update client, consumer, or other person demographic data must integrate with the MCI to ensure their demographic records are registered in the MCI and appropriately merged with matching client records in the index.

Such solutions must integrate with the DOH MCI and ensure the end-users of the solution can leverage the Person service operations to register and maintain their person demographic records in the MCI. This must include interactions that update the MCI when record duplication, deactivation, and similar record management scenarios occur within the scope of the Offeror’s proposed solution.

3.5.2.1 Requirement – Master Client Index (MCI) Integration

The Offeror must integrate their proposed solution with the DOH Master Client Index (MCI) if the Offeror’s proposed solution will store person demographic data of clients, members, beneficiaries, or other individuals who:

- Apply for or receive DOH program services or benefits; or
- Are the subject of a DOH registry; or

- Are a participant in a case, filing-unit, or other group for which DOH expends funds or must measure services.

The Offeror must:

- Indicate whether your proposed solution will include demographic records for individuals.
- Indicate whether your proposed solution will integrate with the DOH Master Client Index.
    - If your solution will not integrate with the DOH MCI, please indicate why.
    - If your solution will integrate with the DOH MCI, please describe your process to register and merge client demographic information records with the MCI.
        - Include the technical approach and the high-level search, create, update, and synchronization procedures for managing MCI relevant demographic data in your solution.

3.5.3 IRIS and ALDER Integration

DOH uses the State of Alaska Enterprise Resource Planning (ERP) system, IRIS, for managing finance, accounting, property-asset, and HR management functions. DOH uses the State of Alaska ALDER data warehouse for reporting and extracting finance, accounting and HR data.
Solutions that include these functions should plan for a gap analysis to determine the appropriate integration approach that avoids duplication of services and addresses developing and integrating complementary solution services and functions.

3.5.3.1 Requirement

Offerors whose proposed solution includes finance, accounting, and HR functions must plan to conduct a gap analysis activity with DOH ITS, DOH Program staff, and Department of Administration Division of Finance IRIS support subject matter experts. This analysis is to determine which system will own which processes, how the systems will integrate and where the data will live.

Offeror’s proposal must include activities to support this gap analysis and associated DDI activities to interface between IRIS, ALDER and the proposed solution.

3.5.4 Authentication and Single Sign On

DOH has established a standard authentication platform, using Microsoft’s Active Directory (AD) to support authentication for DOH hosted systems.

DOH has established a standard federated authentication platform, Microsoft Active Directory Federation Services (ADFS), to support single sign on authentication scenarios for DOH employees who use systems external to the department that cannot integrate with the DOH Active Directory.

Integration with either of these methods provides a uniform authentication mechanism for DOH staff and sponsored external partner/contractor staff to manage authorized access to department information systems. Leveraging the DOH AD allows the Offeror’s solution to inherit the account management, authentication, and audit-logging features of the DOH AD to validate authorized access and meet several technical security controls.

3.5.4.1 Requirement – Single Sign-On and Authentication

The Offeror must integrate their solution with the Alaska DOH Active Directory or DOH Active Directory Federated Services (ADFS). The integration must support authentication access requests prior to authorization.

The Offeror will include cost and activities in their proposal to support the DOH AD integration.

3.5.5 Technical Services and Development Platform

DOH expects the Offeror to align their proposal with this DOH standard technical services platform to the maximum extent possible.

DOH ITS operates a leading software development lifecycle (SDLC) management platform. See IT Reference D for details on this tool. To reduce project overhead and transition costs, the Offeror is encouraged to consider using the DOH artifact version management repository.

3.5.5.1 Requirement – Development Platform

The Offeror will use the software identified in IT Reference D for the development and deployment of this application. The Offeror must state which version the application components are designed in and how this solution will be accessed in the DOH environment. You will need to identify what skills and expertise would be needed to support your proposed infrastructure.

For each non-DOH standard software component in the proposed solution:

- Describe the purpose of the non-standard component;
- Propose a component in the DOH IT standards that could be used instead of the non-standard component;
- Include an optional cost adjustment to implement the solution using that DOH standard component within the cost proposal section of the RFP;
- If there is no DOH standard software component identified that meets the function of the non-standard component proposed, identify a Microsoft component that meets the purpose of the non-standard proposed component;
- Include an optional cost adjustment to implement the solution using that Microsoft component within the cost proposal section of the RFP; and
- If no Microsoft component exists that meets the purpose of the proposed non-standard component, indicate there is no equivalent component available.

3.5.5.2 Requirement – Software Development Lifecycle (SDLC)

The Offeror must apply a methodology that demonstrates key elements of the SDLC, including:

- Gathered and validated requirements and acceptance criteria artifacts;
- Documented and validated design artifacts;
- Documented development and build tools and processes;
- Versioned and managed development artifact change sets;
- Documented deployment and promotion processes for moving builds and release candidates from lower environments to higher-confidence environments and ultimately production (e.g., development > system integration test > user acceptance test > production & training);
- Documented quality assurance, system test, and user acceptance test script and results artifacts;
- Documented release management procedures.

The Offeror must use a set of industry standard tools to track and manage artifacts of the SDLC and must align this toolset with the standard DOH SDLC tools.

3.5.5.3 Requirement – Secure Systems Development Lifecycle

The Offeror must complete software development in compliance with DOH Secure Systems Development Lifecycle, including:

- **Secure Coding** - The Offeror shall disclose what tools are used in the software development environment to encourage secure coding.
- **Disclosure** - The Offeror shall document in writing to the Purchaser all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or proprietary.
- **Evaluation** - The Offeror shall make reasonable efforts to ensure third party software meets all the terms of this agreement and is as secure as the custom code developed under this agreement.
- **Source Code Scanning -** The Offeror shall work with DOH staff to facilitate static code scanning for all product and 3rd party files using a DOH provided scanning solution.
- **Hosting Environment Hardening** – The Offeror shall work with DOH staff to ensure that any hosting environment utilized complies with department adopted standards for security hardening.
- **Vulnerability and Penetration Testing** – for SaaS and XaaS environments, the Offeror shall facilitate requests for 3rd party vulnerability and/or penetration testing of DOH solutions.

3.5.6 DOH Managed Off-site Hosting Scenarios

All DOH Systems Integration and DDI Services and Standards apply to DOH managed off-site hosting scenarios.

3.5.6.1 Requirement

The Offeror must understand and acknowledge 3.5.6.

3.5.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS solutions implicitly provide a limited degree of freedom to deviate from DOH IT Systems Integration and DDI Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS hosting environment, SaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

3.5.7.1 Requirement

When federal funding rights apply, see *section 3.4.4 Software Procurement Assurance – Federal Rights*, the Offeror's proposed solution must employ DOH IT Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska maintenance risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future maintenance risks.

3.6 Systems Operations and Administration Services and Standards

System Operations and Administration Services includes the activities DOH ITS performs to support technical system operations and system administration. This section describes information system administration services that support solutions operating in production.

3.6.1 Administration Services and Standards

DOH ITS operates and manages technical services for DOH information systems and applications. This includes ongoing administration, configuration monitoring and security patching of the underlying software components of the solution.

See IT Reference D for the list of technical service components administered by DOH IT within the System Operations and Administration Services service line.

3.6.1.1 Requirement – Centralized Technical Administration

The Offeror must understand that information technology administration duties are restricted to qualified individuals within the centralized DOH ITS section. DOH Program staff outside the DOH ITS section are not authorized to manage or administer technical information technology services. Examples of technical services include, but are not limited to administration of: relational database management systems (Oracle, SQL Server, MySQL, PostgreSQL, etc.); application servers (ASP.NET, JEE, PHP, etc.), and desktop and server operating systems.

Non-ITS, DOH Program staff may be delegated administration of business services via secured, audited user-interfaces in the application, such as interfaces to create user accounts within the application, assign security roles within the application, maintain code-lookup tables, and other business administration functions. All business administration changes must be completed via a privileged, secured application user-interface that logs all data changes and which user made the change.

The Offeror must validate all technical administration designs with DOH IT stakeholders in the System Operations and Administration Services service line.

The Offeror must include appropriate documentation and training for DOH ITS staff in the technical services administration for the proposed solution.

3.6.1.2 Requirement – Authorized Access

The Offeror must follow DOH standard operating procedures for obtaining and terminating access to DOH facilities and systems. To support proper access management, the Offeror must notify the DOH contract administrator of any personnel transfers or termination of Offeror personnel, including sub-contractors, who possess DOH credentials and/or badges, or who have DOH information system privileges, within fifteen (15) calendar days. Notification must be in writing. This personnel transfer and termination notification requirement may not be extended and does not supersede other Offeror personnel notification requirements with stricter timelines within the contract. (NIST 800-53 r4 PS 07 D)

3.6.2 DOH Managed Off-site Hosting Scenarios

All DOH Systems Operations and Administration Services and Standards apply to DOH managed off-site hosting scenarios.

3.6.2.1 Requirement

The Offeror must understand and acknowledge 3.6.2.

3.6.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH ITS expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

3.6.3.1 Requirement

When federal funding rights apply, *see section 3.4.4*, the Offeror's proposed solution must employ DOH ITS Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

3.7 Information Security Compliance and Privacy Services and Standards

Information Security Compliance and Privacy Services include the activities DOH ITS performs to support legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice. DOH maintains a robust information security compliance and privacy program. This section describes the information security compliance and privacy services and standards applied throughout the lifecycle of each DOH information system.

3.7.1 Data Retention/Destruction

Destruction of Electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII) on electronic media requires that the organization employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

3.7.1.1 Disposing of Printed Information

All protected printed media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the NIST Special Publication 800-88 Revision 1 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

3.7.1.2 Disposing of Information on Electronic Media

All protected electronic media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the Department of the Army's brief, Cybersecurity: Sanitization of Media (https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6681_Pam25-2-8_WEB_FINAL.pdf#:~:text=The%20procedures%20in%20this%20chapter%20establish%20the%20requirement,the%20disposal%20and%20handling%20of%20hazardous%20IT%20waste) and NIST Special Publication 800-88 Revision 1 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf). Disposed of electronic media must receive a Certificate of Media Disposal or agreed upon proof of disposal for each device disposed.

3.7.1.3 Requirement – Record Retention

The Offeror must comply with the DOH policies and procedures for record retention and disposal of sensitive information (IT Reference F—Data Destruction Information and References), if applicable.

3.7.1.4 Requirement – Data Destruction

The Offeror must provide procedures and agree to all data (including test data) destruction when contract ends if continuing operations and maintenance is not provided by the contractor.

3.7.2 Security Controls

Department, State, and Federal security standards are enforced through State of Alaska and DOH policy and procedure. The procedures leverage FIPS 199 information security categorization and NIST 800-53 information security controls documentation. The DOH Governance, Risk, and Compliance system serves as the system of record to capture this documentation in an "authorization package".

3.7.2.1 Requirement – Authorization Package

Within the proposed scope of work and activities, the Offeror must:

- Work with the Department Security Office (DSO) to document the approach, methodology, roles, responsibilities, processes, and tasks the Offeror will assume to complete the authorization package;
- Develop and submit a complete Authorization Package for review and approval by the DSO;
- Submit to the DOH Security Designee, a thoroughly completed Authorization Package for review and comment within four (4) weeks of the project's initiation and receipt of the Authorization Package questionaire.
    - Offeror shall respond to clarification questions within two (2) weeks of receipt of DOH comments on the Authorization Package.

Security controls are reviewed for risk regardless of whether an application/solution is hosted on premise or elsewhere. A paper version of the Authorization Package is included in IT Reference H – DOH Sample Security Authorization Package.

3.7.2.2 Requirement – Code Vulnerability Scanning

DOH employs a code vulnerability scanning engine. The Offeror shall process all scannable code through the DOH static code vulnerability scanning engine. Findings from the code vulnerability scan will be attached to the systems Authorization Package for review and acceptance from the DOH Department Security Office (DSO).

3.7.2.3 Requirement – Security Control Verification

After the Authorization Package is complete, it is subject to review and acceptance from the DOH Department Security Office (DSO). Approval to operate in the DOH environment is predicated on acceptance of the Authorization Package responses as well as compliance with the processes outlined in *section 3.5.5.3* of this document. These processes may require changes and updates to the system by the Offeror in order to comply with regulatory requirements.

The Offeror must plan activities to work towards security compliance requirements and accommodate an appropriate number of remediation cycles to address any identified defects.
Please note, although workload varies in proportion to the size of the solution, we have found that most small to medium size solutions require 80 to 120 hours to complete the initial security control responses.

3.7.2.4 Requirement – Business Associate Agreement

If data is determined to be ePHI, the DOH Business Associate Agreement must be signed at contract. Other types of data must be treated with appropriate confidential data handling and may be covered by a data usage agreement.

3.7.2.5 Requirement – Authority to Operate

Once all security compliance is established via an approved Authorization Package and signed Business Associate Agreements (BAA) or data usage agreements (as applicable), the solution will be granted an Authority to Operate (ATO) by the DOH designated Division Data Owner, the Department Chief Information Security Officer, and the OIT Department Technology Officer for DOH. The Offeror must plan activities and milestones that support obtaining the ATO prior to production rollout.

The Offeror must plan for delays associated with a solution's inability to initially obtain ATO. These delays must take into consideration the business's implementation targets. It is imperative that authorization package responses be scheduled with ample time for completion, DSO review, and mitigation to not negatively affect the business's implementation targets.

3.7.3 Auditing and Logging Integration

For logging and audit, DOH uses an industry standard Security Information and Event Management (SEIM) system. All systems are required to be capable of logging and auditing in a concise summary that can be easily integrated into the DOH SEIM. The package produced by the application must be inclusive of all the data for who is accessing, reading, and writing data.

3.7.3.1 Requirement

The Offeror's proposed solution must integrate with DOH's SEIM infrastructure. The Offeror's proposed solution must include activities to collaborate with DOH ITS in establishing log collection activities for standard log formats and customizing log parsing for non-standard log formats.

3.7.4 Data Security

Sensitive and/or confidential data includes (but is not limited to) 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, Personal Information (PI) as defined in the State of Alaska Personal Information Protection Act (APIPA), and Payment Card Information (PCI) as defined by Payment Card Industry Data Security Standard (PCI DSS), and Criminal Justice Information (CJI) as defined by the Federal Bureau of Investigation.

3.7.4.1 Requirement

The Offeror's proposed solution must include, define how they will ensure all sensitive, confidential, and/or restricted data is encrypted in-transit and at-rest. Criminal Justice Information Systems (CJIS) and those systems requiring MARS-E compliance must meet these encryption requirements using a FIPS 140-2 certified product.

DOH owns the data and can demand it at any time. Proposed solutions that leverage public or private data sources resulting in DOH business decisions – especially where the business decision reflects a DOH legal jurisdiction related to due process – must ensure DOH retains access to all the data required to support the decision.

3.7.4.2 Requirement

The Offeror's proposed solution must include, define, and validate the capabilities to return DOH owned data to DOH.

Recovery Point Objective (RPO) refers to the maximum amount of data loss – typically defined in terms of time – that may occur in the event of a system failure and consequent rollback to a known consistent state. *Recovery Time Objective* (RTO) refers to the maximum time that may pass between the point in time when a system failure occurs and the point in time when the system is recovered.

3.7.4.3 Requirement – Recovery Point and Recovery Time Objectives

The Offeror's proposed solution must include and define RPO and RTO capabilities. If there are cost-add RPO and RTO capbilities available that exceed the assumptions, scope and cost of your proposal, please identify those options.

3.7.5 Integration Security Controls

When system interfaces (data exchange between systems) and integration requirements exist for a system, integration security controls must be documented and implemented to ensure the confidentiality, integrity and availability of the data for all valid business consumers. To simplify the DOH operating environment, and ensure that many of the required controls are met at the least cost, DOH has implemented an Enterprise Service Bus (ESB) and partnered to leverage the Alaska Health Information Exchange (HIE). Both the ESB and the HIE provide architectural system integration and data exchange services that can be leveraged for re-use by On-DOH premise and Off-site hosted information systems.

3.7.5.1 Requirement

The Offeror must demonstrate leveraging existing DOH security control investments by integrating with DOH systems via the DOH ESB and/or the statewide HIE.

The Offeror must complete and submit to the DSO for review, one Interface Risk Assessment Worksheet, per interface, outlining the specifications and security components of said interface.

3.7.6 DOH Managed Off-site Hosting Considerations

All DOH Information Security Compliance and Privacy Services and Standards apply to DOH managed off-site hosting scenarios.

3.7.6.1 Requirement

The Offeror must understand and acknowledge 3.7.6.

3.7.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH IT Information Security Compliance and Privacy Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment. SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation provided those infrastructure and platform components meet the security compliance requirements of the information managed by the SaaS/XaaS, and if applicable, the requirements in the DOH Business Associate Agreement.

The Offeror's SaaS/XaaS proposal should include encrypting and securing any confidential data, and adopting the latest security measures available to prevent unauthorized access. Security controls include patching application/operating system/firmware, minimizing administrative controls, and completing a DOH Authorization Package and submitting the Authorization Package to our department security office for review and approval, per the requirements under section 3.7.2. The authorization package must be approved before systems or applications are authorized for production. The Offeror assumes the responsibility for any and all authentication and account creations or modifications.

3.7.7.1 Requirement – SaaS/XaaS Security Responsibilities

Proposals for SaaS/XaaS offerings should include a clear delineation of the system's security mechanisms and configurations the Offeror will be responsible for, and those for which DOH will be responsible.

The Offeror is also responsible for service patching and completing an RSA Authorization Package.

3.7.7.2 Requirement – SaaS/XaaS Logging and Auditing

For proposals that include SaaS/XaaS solutions that may manage confidential data, the SaaS/XaaS must include a logging and auditing solution. All components and systems within the Offeror's proposal are required to be capable of logging all data access requests to read or write data, including the requesting user id. The audit-log data that is produced by the application must include all the data to identify who created, accessed, updated, and deleted data and when each event occurred.

The application must be readily capable of generating logging and auditing reports 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, including how responsible DOH entities (DSO, Division Data Owner) will be able to access it to perform oversight related tasks.

3.8 Enterprise Desktop and Mobility Services and Standards

Enterprise Desktop and Mobility Services include the activities DOH ITS performs to define, deploy, and support the DOH enterprise desktop and mobility endpoints. DOH maintains an enterprise desktop for all datacenter and field-deployed hosts. The desktop is based on a golden image, created and maintained based on input from the integration and development, information security, and operations service lines and standards. This section describes the procurement relevant enterprise desktop services and standards used to manage and maintain DOH end-user desktops.

3.8.1 Desktop Access and Configuration

DOH utilizes Dell workstation and server hardware. Offerors should propose solutions that are device independent. The DOH Enterprise Desktop is a supported version of Microsoft Windows, with the supported web browser, productivity suite and other common, standard or approved software components and applications. See IT Reference D for currently supported hardware and operating system(s).

DOH is a least privilege environment and staff are not granted elevated privilege without individually reviewed and approved security policy waivers. DOH Program staff work with DOH ITS to request, review, and determine compatibility, redundancy, and fit of non-standard software. DOH Program staff are not permitted to install, nor can they independently authorize the installation of, new software components or applications on the desktop. Offerors should avoid solutions that require customization of the DOH Enterprise Desktop.

If the Offeror's proposed solution requires use of a desktop web browser, the solution must be browser independent and be fully capable of functioning with the standard browser in the DOH Enterprise Desktop Standards. See IT Reference D for currently supported web browser version(s).

If the Offeror's proposed solution requires use of desktop productivity suite software, the solution should be fully capable of functioning with the standard desktop suite in the DOH Enterprise Desktop Standards. See IT Reference D for currently supported desktop productivity software.

3.8.1.1 Requirement – Desktop Access and Configuration

The Offeror must propose a solution that supports the DOH currently deployed desktop operating system (OS) and does not require elevated privileges for the end-user on their desktop. The Offeror must include activities in their proposal to establish whether each and every end-user desktop software component required to support the proposed solution is a part of the standard DOH Enterprise Desktop. The Offeror must include activities in their proposal to work with the DOH Enterprise Desktop team to integrate each non-standard software component. These activities must include working with DOH Enterprise Desktop service line staff to:

- Accept or identify acceptable alternatives for each non-standard software component.
- Establish installation, configuration, and support procedures for each non-standard software component.

3.8.1.2 Requirement – Web Browser Compatibility

The Offeror must plan to support proposed solution compatibility with DOH' currently deployed web browser version(s). The required functionality of the solution must be fully supported, or the Offeror must include in their proposal the plan, cost, and activities to make the proposed solution fully supported. The Offeror must review the DOH standard browser vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any browser versions that will become unsupported during the execution of the contract (per the vendor's published support lifecycle material).

3.8.1.3 Requirement – Desktop Productivity Software Compatibility

The Offeror must plan to support DOH currently deployed desktop productivity suite version(s). The Offeror must review the DOH standard desktop productivity suite vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any versions of productivity suite software versions that will become unsupported during the planned execution of the contract (per the vendor's published support lifecycle material). The Offeror must include in their cost proposal, the optional contingency cost of one unanticipated productivity suite software version compatibility upgrade for the proposed application.

3.8.1.4 Requirement – Other Desktop Software and Components

The Offeror must delineate all the desktop software, access, and configuration requirements of the application not addressed elsewhere in the Enterprise Desktop Services and Standards section.

3.8.2 Mobile Devices and Tablets

Mobile devices for DOH are:

- Dell Windows based Tablets
  - Configured with the latest version of Microsoft Standard browsers
  - Web applications are to be Browser version independent which means they support current versions of Internet browsers for Microsoft, FireFox, and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.
- Apple iOS based Tablets and Smart Phones
  - Configured with the latest version of Safari and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.

Dell and Apple Devices are configured with the latest operating systems or 1 version previous.

The DOH mobile device strategy is evolving rapidly and is not stable or complete for supporting the ability to store or transmit confidential data. If their solution includes mobile device end-points, Offerors should plan for extensive engagement with the DOH Enterprise Desktop and Mobility service line

3.8.2.1 Requirement

The Offeror must plan appropriate activities to support mobile device endpoint integration. These activities must include selecting and adapting mobile solution software components to a DOH standard mobile device that supports all security compliance requirements of the data being stored on or transmitted to/from the mobile device endpoints.

3.8.3 DOH Managed Off-site Hosting Scenarios

All DOH Enterprise Desktop and Mobility Services and Standards apply to DOH desktops managed off-site hosting scenarios.

3.8.3.1 Requirement

The Offeror must understand and acknowledge 3.8.3.

3.8.4 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ embedded, non-compliant, end-user desktops within the SaaS/XaaS, provided that:

(a) Equivalent desktop security controls are proposed and implemented to those present on the DOH Enterprise Desktop, and
(b) The SaaS/XaaS supports DOH Enterprise Desktop supported standard software for accessing SaaS solution desktops. See IT Reference D for supported software.

3.8.4.1 Requirement

When federal funding rights apply, *see section 3.4.4*, the Offeror's proposed solution must employ DOH ITS Enterprise Desktop Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

3.9 DOH Hosting and Datacenter Services and Standards

DOH Hosting and Datacenter Services include the activities DOH ITS performs to design, implement, and operate standard information technology infrastructure and platform offerings in DOH managed datacenters. This includes both the primary DOH data centers in Juneau and Anchorage, as well as satellite facilities in secondary locations that require similar services to meet disaster recovery and business continuity requirements. Relying on robust, appliance style hardware with advanced storage area network data deduplication and replication functions, advanced firewalls, and virtualized host infrastructure, DOH datacenter infrastructure provides the flexibility to rapidly deploy new hosts in a physically and logically secure environment.

Please see the DOH Hosting and Datacenter Service Standards section of Reference D - Information Technology Standards,

3.9.1 On-DOH Premise Hosting Considerations

DOH provides and maintains a standardized set of infrastructure and platform services to deliver a full-service private cloud offering, leveraging the State of Alaska Wide Area Network to span two geo-redundant data centers located in Juneau and Anchorage.

3.9.1.1 Requirement

Proposals for hosting the solution on the State network should include the responsibilities and communication process for DOH IT for development, test, and production environments and follow DOH directives for migration to production.

The Offeror will not have direct access to the production environment on the State Network and must work through the appropriate protocols to effect change appropriately. The Offeror must work with DOH IT for all security mechanisms, including patching updates.

3.9.1.2 Requirement

The Offeror will use the software identified in IT Reference D for the hosting of this application. The Offeror must state which version the application components are implemented in and how this solution will be accessed in the DOH environment. The Offeror will need to identify what skills and expertise would be needed to support the proposed infrastructure.

3.9.2 DOH Managed Off-site hosting considerations

All DOH Hosting and Datacenter Services and Standards must be followed and applied to DOH managed off-site hosting scenarios.

3.9.2.1 Requirement

The Offeror must understand and acknowledge 3.9.2.

3.9.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH Hosting and Datacenter Services and Standards do not support Software as a Service (SaaS) or Anything as a Service (XaaS) offerings. Offerors proposing SaaS/XaaS solutions must provide and manage their own hosting and datacenter services. Offerors may subcontract these hosting and datacenter services, provided appropriate security agreements, such as a Business Associate Agreement or data usage agreement, are in place for the data being stored in or transported to/from the subcontracted hosting datacenter.

3.9.3.1 Requirement

The Offeror must understand and acknowledge 3.9.3.

3.10 DOH Wide Area Network, Telecommunications, and Perimeter Security Services and Standards

DOH Wide Area Network, Telecommunications and Perimeter Security Services include the activities DOH IT performs to integrate the DOH LAN with the State of Alaska (SOA) wide area network, telecommunications and perimeter security managed by Department of Administration (DOA) Office of Information Technology (OIT). These services are built upon a layered architecture design that includes VPN, ingress/egress, network address translation and port address translation services and capabilities provisioned, managed, and maintained by OIT. To maximize the security capabilities of these services and ensure systems maintain compliance with system security requirements and industry standards, DOH ITS and OIT follow strict change management processes that include reviews and approvals for all information systems and applications changes that impact WAN, Telecommunications, and Perimeter Security. See 3.7 Information Security Compliance and Privacy Services and Standards for additional details regarding security compliance. Work and service requests reflecting these changes are managed via an OIT ticketing system (Reference D, section DOH Wide Area Network, Telecommunications and Perimeter and WAN Security Service Standards).

3.10.1 State WAN and Bandwidth

The State Wide Area Network (WAN) is maintained at the enterprise level by the Department of Administration (DOA)/Office of Information Technology (OIT); WAN connectivity and bandwidth available to grantees via the WAN is controlled by contractual agreements between OIT and local internet providers. Some rural areas experience internet connection speed as low as 56k and frequent network disruptions. Changes to the State WAN, for example new ingress points, IPSEC tunnels, etc., require both DOH IT Security Office and DOA State Security Office review and approval.

Due to the great distances between communities in Alaska and the lack of road connections in most areas of the state, electrical power is locally generated in most parts of the state. While Anchorage has redundant transmission lines from its electrical generating plant and rarely experiences system-wide outages, local outages can occur due to weather-related conditions or damage to the distribution system. Electrical power in most other parts of the state is subject to periodic system-wide outages as well as localized outages. Broadband service is available in most of the larger communities in Alaska. However, in communities located off the road system that rely on satellite connections, a T1 line is a significant expense.

3.10.1.1 Requirement

The Offeror must understand and acknowledge Bandwidth constraints and denote any performance degradation that could be encountered by their solution and suggested mitigations. Offeror must note any services requiring communications outside the State of Alaska WAN.

3.10.2 DOH Managed Off-site Hosting Scenarios

DOH operates only within the State of Alaska Wide Area Network and uses only State of Alaska provided telecommunications services. Proposals requiring new State of Alaska Wide Area Networks or telecommunications (phone, fax, etc.) services must be approved by the OIT Department Technology Officer.

3.10.2.1 Requirement

The Offeror must understand and acknowledge 3.10.2.

3.10.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

Offerors proposing SaaS/XaaS solutions must provide and manage their own Wide Area Network and telecommunications services to support any required network and telephony services of the proposed solution. The proposed solution must grant access to the DOH Program staff via a supported DOH desktop web-browser, or a desktop thin client, or similar DOH approved and supported software. See Reference D - Information Technology Standards.

3.10.3.1 Requirement

The Offeror must understand and acknowledge 3.10.3.

3.11 Accessibility

Alaska Administrative Orders 262 and 129 establish the Americans with Disabilities Act (ADA) compliance program in accordance with the American with Disabilities Act (42 U.S.c. 12101 et seq.). DOH expects the Offeror to propose and deliver solutions that meet the Alaska ADA program.

3.11.1 ADA Compliance for Access to Information Systems and Applications

DOH requires ADA compliant application access.

Two important resources provide guidance for web developers designing accessible web pages. One is the Section 508 Standards, which Federal agencies must follow for their own new web pages. To learn more about the Section 508 Standards the Access Board maintains information on its website at www.access-board.gov.

The second is the General Services Administration information for web developers interested in accessible web design at https://www.gsa.gov/technology/build-websites-and-digital-services. This information was developed in conjunction with the Access Board, the Department of Justice, and the Department of Education
A more comprehensive resource is the Web Content Accessibility Guidelines developed by the Web Accessibility Initiative. These guidelines help designers make web pages as accessible as possible to the widest range of users, including users with disabilities. The Web Accessibility Initiative is a subgroup of the World Wide Web Consortium — the same organization that standardizes the programming language followed by all web developers.

Information for web developers interested in making their web pages as accessible as possible, including the current version of the Web Content Accessibility Guidelines (and associated checklists), can be found at https://www.w3.org/WAI/standards-guidelines/wcag/.

3.11.1.1 Requirement

DOH requires that web pages and web applications be accessible for ADA compliance. This includes online forms and tables which must be made so that those elements are accessible. Documents on the website must be provided in HTML or a text-based format in addition to any other formats.

It is the responsibility of the Offeror to ensure that the web page\web application features are ADA compliant.

3.12 State of Alaska DOH MITA Standards and Department IT Technology Standards

The Department is migrating toward an enterprise Service Oriented Architecture (SOA) consistent with Medicaid Information Technology Architecture (MITA) and the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards (7C&S) outlined below:

- Modularity
- MITA Condition
- Industry Standards Condition
- Leverage Condition
- Business Results Condition
- Reporting Condition
- Interoperability Condition

3.12.1 MITA Requirements

The Offeror’s proposal must respond to the questions on how their solution addresses or does not address each of the 7C&S.