Information Technology Requirements

State of Alaska

Department of Health & Social Services

TABLE OF CONTENTS

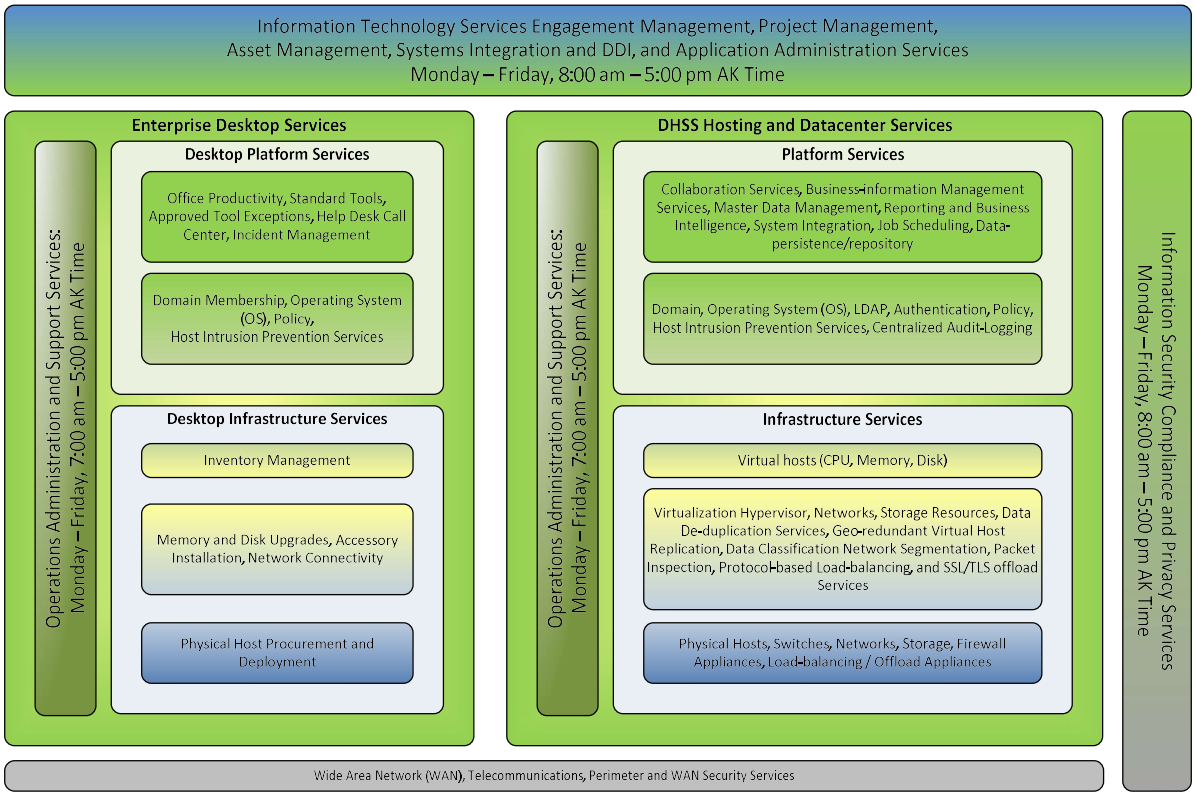
1 Purpose of IT Requirements

The State of Alaska Department of Health and Social Services (DHSS) has adopted the Medicaid Information Technology Architecture (MITA) standards and has 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 include addressing how and if the proposed product solution will integrate into this environment and not be a standalone system.

1.1 IT Services Organization Summary

DHSS Division of Finance and Management Services (FMS) Information Technology Services (ITS) section operates a full-service information technology services organization within DHSS. As the diagram below indicates, this includes:

Service Line	Description
Engagement and Service Delivery Management	Services to engage with customers and manage delivery of all IT services
Project Portfolio Management	Services to support project management enterprise process development and execution
Asset Management	Services to manage software licensing and other software and information assets
Systems Integration and DDI	Services to support system architecture development, integration between DHSS systems and information system design, development and implementation
Systems Operations and Administration	Services to support technical system operations and system administration
Information Security Compliance and Privacy	Services to support legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice
Enterprise Desktop and Mobility	Services to define, deploy and support the DHSS enterprise desktop and mobility endpoints
DHSS Hosting and Datacenter	Services to design, implement and operate standard information technology infrastructure and platform offerings
DHSS Wide Area Network, Telecommunications and Perimeter Security	Services to integrate the DHSS 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)



1.2 IT Requirements Intent and Approach

The Offeror should understand the intent and approach of the IT Requirements. DHSS ITS values our partner relationships with external vendors, contractors and grantees. DHSS ITS is focused on providing the best value to our customers by supporting IT procurements from the RFP solicitation process all the way 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 provide key operational insights into DHSS ITS service delivery approach to help Offerors understand the DHSS ITS organization they are proposing to engage with, and to give Offerors the opportunity to shape their proposals to best fit the team of DHSS program, DHSS ITS, and Offeror staff that will work together to deliver the solution.
2. The requirements identify specific answerable requirements statements and questions that Offerors must meet for responsiveness.

To meet those two goals, the IT requirements are structured into services and standards sections corresponding to a service line view of the DHSS ITS organization. For example, the solicitation-relevant services and requirements for end-user desktop configurations are located in the “Enterprise Desktop Services and Standards” section.

DHSS IT recognizes that Offerors may consider proposing one or more of the following options:

- DHSS hosted and managed solution components;
- 3rd party hosted, DHSS managed solution components;

- Software as a Service (SaaS) and Anything as a Service (XaaS) 3rd party hosted, 3rd party managed solution components. Software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. XaaS is a general, collective term that refers to the delivery of anything as a service. It recognizes the vast number of products, tools and technologies that vendors now deliver to users as a service over a network -- typically the internet -- rather than provide locally or on-site within an enterprise.

To support these scenarios, each service and standards section includes subsections that apply to all procurements, plus two specific subsections to address variations and exceptions for “DHSS Managed Off-site Hosting Scenarios” and “Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios”.

Offerors should read each section carefully to understand how DHSS ITS applies a particular service-line to procured services and what specific requirements questions and statements must be answered.

2 Technical Qualifications Response

2.1 Minimum Qualifications

Offerors must complete **Required Vendor Response - DHSS 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 DHSS Technology Services, Standards and IT Road Map

Information technology services for DHSS agencies are provided by DHSS Division of Finance and Management Services (FMS) Information Technology Services (ITS). DHSS ITS provides the following functions: maintenance of the DHSS Data Centers in Juneau and Anchorage; project execution support; operational support; and integration assistance for systems hosted on site.

~~3.1 DHSS Information Technology Services Staffing Support~~

This section intentionally removed.

~~3.1.1 DHSS IT General Staffing Support Model Defined~~

This section intentionally removed.

~~*3.1.1.1 Requirement*~~

This section intentionally removed.

~~3.1.2 DHSS ITS Project Staffing Support Model Defined~~

This section intentionally removed.

~~*3.1.2.1 Requirement*~~

This section intentionally removed.

~~3.1.3 DHSS On-going Operations Staffing Support Model Defined~~

This section intentionally removed.

~~*3.1.3.1 Requirement – Offeror-managed production operations phases*~~

This section intentionally removed.

~~*3.1.3.2 Requirement – DHSS-managed Production Operations Phases*~~

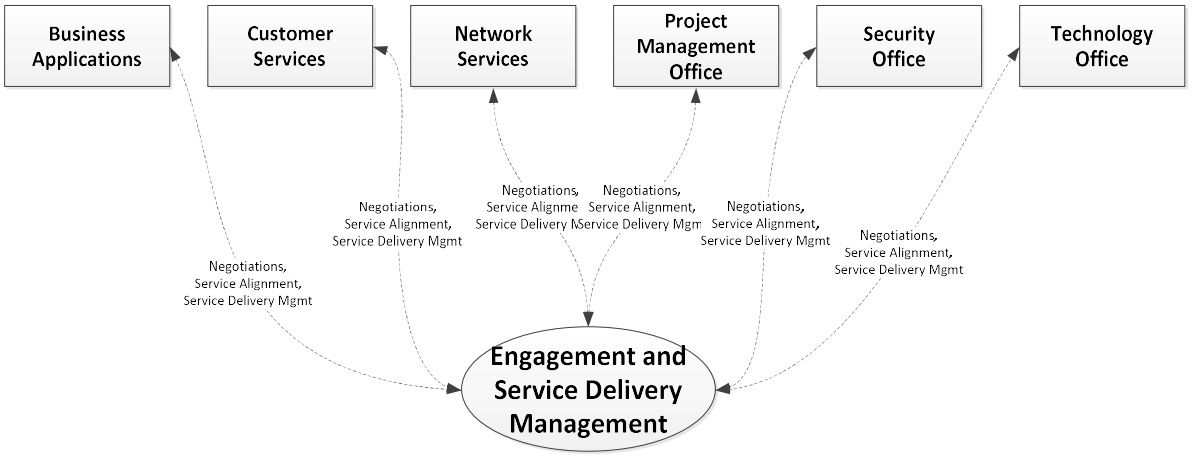
This section intentionally removed.

3.2 Engagement and Service Delivery Management Services and Standards

Engagement and Service Delivery Management Services includes the activities DHSS ITS performs to engage with our DHSS Program staff, and manage delivery of all IT services. This includes defining the

needs, assisting with DHSS IT Governance needs alignment and change request processes, and applying and managing the correct DHSS ITS service-lines for specific DHSS ITS initiatives and procurements.

Engagement and Service Delivery Management Services is matrixed per the following organizational mapping:



3.2.1 Contract Negotiations ITS Review and Approval

DHSS 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 DHSS ITS, Procurement and DHSS Program staff to review and approval all IT related contract elements.

3.2.2 Project Kickoff Service Alignment Conference

As part of project kickoff activities, DHSS ITS and Program representatives will meet with the Offeror's execution team to agree upon the necessary DHSS 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 DHSS 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 DHSS ITS does not support, DHSS ITS staffing resource constraints, or other gaps. See IT Reference B—DHSS Project Management Requirements "Project Initiation/Kick Off meeting" for information about additional project kick off activities.

3.2.2.1 Requirement – DHSS ITS Service Alignment Conference

The Offeror must include project activities to reach agreement with DHSS ITS and DHSS Program staff on DHSS 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 DHSS Service Line Engagement and Planning

DHSS ITS recognizes that different procurements require customized support activities to succeed within scope, schedule, and resource constraints. To quickly align with a given procurement's constraints and

ensure the best outcome, the DHSS ITS service lines identified to support the procurement will work with DHSS Program 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 – DHSS IT Service Line Engagement and Planning Workshops

The Offeror must include project activities to reach agreement with DHSS ITS and DHSS Program staff representatives on the DHSS ITS service line engagements from DHSS ITS service lines 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 DHSS Service Line Management Processes and Tools~~

This section intentionally removed.

~~*3.2.4.1 Requirement – Service Line Management Processes and Tools Alignment*~~

This section intentionally removed.

~~3.2.5 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.2.5.1 Requirement*~~

This section intentionally removed.

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

All DHSS 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 DHSS Engagement and Service Delivery Management Services and standards apply to Software as a Service (SaaS) and Anything as a Service (XaaS) scenarios.

3.3 Project Portfolio Management Services and Standards

See IT Reference B—DHSS Project Management Requirements.

3.3.1 DHSS Managed Off-site Hosting Scenarios

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

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

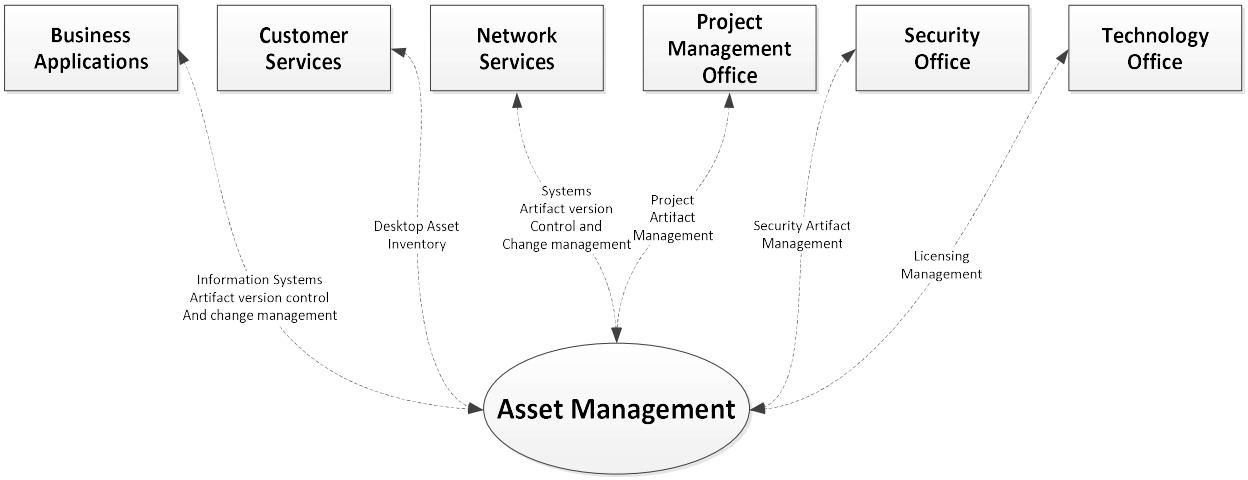
All DHSS Project Portfolio Management Services and Standards apply to SaaS/XaaS scenarios.

3.4 Asset Management Services and Standards

Asset Management Services includes the activities DHSS ITS performs to manage software licensing and other software and information assets. DHSS considers data, software source code, configuration files,

binaries, licenses and configured systems all as “assets”. DHSS 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 and procedures to ensure individual assets are identified and version consistent artifact sets can be recreated to support disaster recovery, testing, audit and other scenarios.

DHSS Asset Management Services supports other DHSS ITS service lines through processes and tools that implement version control, software license inventory and software procurement assurances. Asset Management Services is matrixed per the following organizational mapping:



~~3.4.1 Artifact Version Management~~

This section intentionally removed.

~~3.4.1.1 Requirement~~

This section intentionally removed.

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

The contractor must convey to DHSS, 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~~

This section intentionally removed.

~~*3.4.3.1 Requirement*~~

This section intentionally removed.

~~3.4.4 Software Procurement Assurance – Federal Rights~~

This section intentionally removed.

~~*3.4.4.1 Requirement*~~

This section intentionally removed.

3.4.5 Data Ownership

3.4.5.1 Requirement – Data Ownership

DHSS 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 DHSS information are the sole and exclusive property of DHSS. The Offeror agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from DHSS. Offeror agrees to abide by all federal and state confidentiality requirements.

In addition, the Offeror agrees to provide to DHSS, 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 as agreed upon by both parties.

~~3.4.6 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.4.6.1 Requirement*~~

This section intentionally removed.

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

Software as a Service (SaaS) and Anything as a Service (XaaS) delivery models afford DHSS the ability to leverage the business value of information management 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.

DHSS ITS expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DHSS ITS Asset Management Services and Standards. Specifically, when federal funding rights do not apply, and when DHSS is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may avoid the requirement to transfer source code artifacts identified in *section 3.4.1*.

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.

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 DHSS and the Offeror to ensure that all DHSS data will be returned to DHSS in a cooperative manner at the close of the contract or the decommissioning of the solution. DHSS data may include deliverables, reports, configuration details, business requirement documents, test plans, scripts, and results.

~~3.5 Systems Integration and DDI Services and Standards~~

This section intentionally removed.

~~3.5.1 Information Exchange Architecture~~

This section intentionally removed.

~~*3.5.1.1 Requirement*~~

This section intentionally removed.

~~3.5.2 Master Data Management~~

This section intentionally removed.

~~*3.5.2.1 Requirement – Master Client Index (MCI) Integration*~~

This section intentionally removed.

~~3.5.3 IRIS and ALDER Integration~~

This section intentionally removed.

~~*3.5.3.1 Requirement*~~

This section intentionally removed.

~~3.5.4 Authentication and Single Sign On~~

This section intentionally removed.

~~*3.5.4.1 Requirement – Single Sign On*~~

This section intentionally removed.

~~*3.5.4.2 Requirement – DHSS ADFS Based Single Sign On for SaaS/XaaS and managed Commercial Off the Shelf (COTS)*~~

This section intentionally removed.

~~3.5.5 Technical Services and Development Platform~~

This section intentionally removed.

~~*3.5.5.1 Requirement – Development Platform*~~

This section intentionally removed.

~~*3.5.5.2 Requirement – Software Development Lifecycle (SDLC)*~~

This section intentionally removed.

~~*3.5.5.3 Requirement – Secure Development Lifecycle (SecDLC)*~~

This section intentionally removed.

~~3.5.6 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.5.6.1 Requirement*~~

This section intentionally removed.

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

This section intentionally removed.

~~*3.5.7.1 Requirement*~~

This section intentionally removed.

~~3.6 Systems Operations and Administration Services and Standards~~

This section intentionally removed.

~~3.6.1 Administration Services and Standards~~

This section intentionally removed.

~~*3.6.1.1 Requirement – Centralized Technical Administration*~~

This section intentionally removed.

~~*3.6.1.2 Requirement – Authorized Access*~~

This section intentionally removed.

~~3.6.2 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.6.2.1 Requirement*~~

This section intentionally removed.

~~3.6.3 Software as a Software as a Service (SaaS) and Anything as a Service (XaaS) Scenario~~

This section intentionally removed.

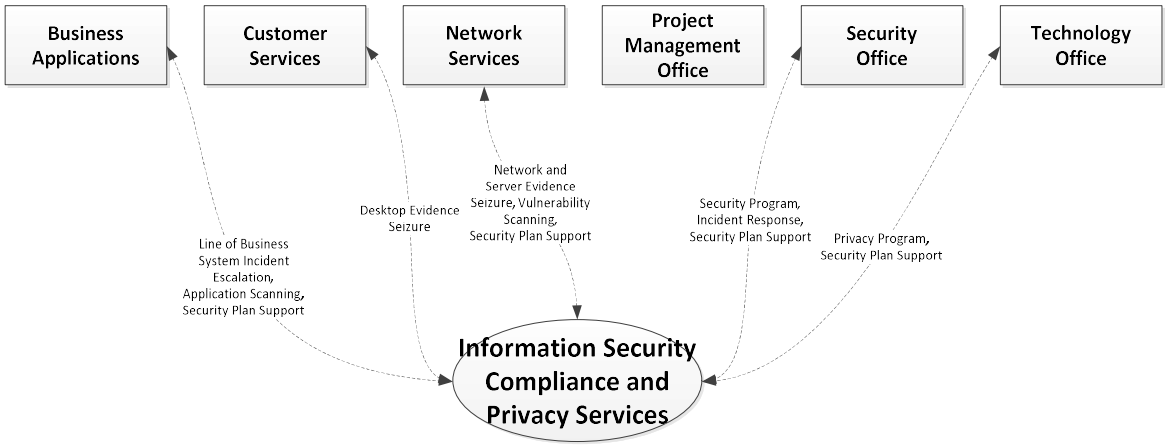
~~*3.6.3.1 Requirement*~~

This section intentionally removed.

3.7 Information Security Compliance and Privacy Services and Standards

Information Security Compliance and Privacy Services include the activities DHSS ITS performs to support legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice. DHSS 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 DHSS information system.

Information Security Compliance and Privacy Services is matrixed per the following organizational mapping:



3.7.1 Data Retention/Destruction

Destruction for Electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII) on electronic media includes: clearing (using software or hardware products to overwrite media with non-sensitive data); purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains); or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

3.7.1.1 Disposing of Printed Information

Approved techniques for disposing of printed information containing Electronic Protected Health Information (ePHI) or Personal Information (PII) include:

- Using a cross-cut shredder
- Incineration

3.7.1.2 Disposing of Information on Electronic Media

Approved techniques for disposing of information on fixed and removable media containing Electronic Protected Health Information (ePHI) or Personal Information (PII):

- Securely erase the media
    - DBAN the media or use Drive eRazer Pro
    - The technician who securely erased the media shall sign the Media Disposal Assurance Form (MDAF) (http://doa.alaska.gov/dgs/property/pdf/Media%20Disposal%20Assurance%20Form.pdf)
    - The technician's supervisor shall sign the MDAF
    - A copy of the signed Media Disposal Assurance Form shall be attached to the Transfer Authorization Form (TAR) that accompanies the salvaged/surplus device(s), prior to acceptance by the Property Manager or State Warehouses.
- Destruction of fixed media may be done using the following techniques only when secure erase is not technically feasible:
    - Magnetic Platters drilled or Magnetic Platters removed and broken
    - The technician who destroyed the fixed media shall sign the Media Disposal Assurance Form (MDAF) (http://doa.alaska.gov/dgs/property/pdf/Media%20Disposal%20Assurance%20Form.pdf)
    - The technician's supervisor shall sign the MDAF
- Destruction of removable media may be done using the following techniques only when a secure erase is not technically feasible:
    - Magnetic media severed or broken
    - If applicable, the technician who destroyed the removable media shall sign the Media Disposal Assurance Form (MDAF) (http://doa.alaska.gov/dgs/property/pdf/Media%20Disposal%20Assurance%20Form.pdf)
    - If applicable, the technician's supervisor shall sign the MDAF

3.7.1.3 Requirement – Record Retention

The Offeror must comply with the DHSS policies and procedures for record retention (http://archives.alaska.gov/records_management/schedules/hss_retention.html) 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 DHSS policy and procedure. The procedures leverage FIPS 199 information security categorization and NIST 800-53 information security controls documentation. The DHSS Archer GRA system serves as system of record

to capture this documentation in an "authorization package". The Offeror must coordinate with the Department Security Office (DSO) to document the approach, methodology, roles and responsibilities, processes and tasks the Offeror will assume to complete the authorization package.

All sensitive, confidential, and/or restricted data is encrypted in-transit and at-rest. Criminal Justice Information Systems (CJIS) must meet these encryption requirements using a NIST FIPS 140-2 certified product.

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).

Security controls are audited for the DHSS Risk Assessment regardless of whether an application/solution is hosted on premise or elsewhere. DHSS Security standards plus a sample paper version of the RSA Archer Authorization Package are included in IT Reference H – DHSS Sample Security Authorization Package – Moderate Control Set.

3.7.2.1 Requirement – Authorization Package

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

- A complete Archer Authorization Package for review and approval by the state.
- The Authorization Package shall be compliant with, and reference (where appropriate) all State (enterprise) and DHSS IT Security Policies and all applicable State and Federal IT legislation. DHSS will facilitate the development and approval of the plan.

The Master Project Management Plan will detail the Offeror's approach to all facets of security in relation to the proposed application. This should include listings of detailed tasks with task descriptions and schedules. The Offeror shall submit to the DHSS Project Manager draft versions of each Authorization Package for review and comment within four (4) weeks of the project's initiation and gaining access to the RSA Archer system. DHSS comments shall be returned to the Offeror two weeks later. Offeror shall submit a final Authorization Package within two (2) weeks of receipt of DHSS comments on the draft Authorization Package.

The DHSS Business Associate Agreement or data usage agreement must be signed at contract award in accordance with IT Reference H:

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

3.7.2.2 Requirement – Security Control Verification

After the Authorization Package is complete it is subject for review and acceptance from the DHSS Department Security Office (DSO) and Department of Administration (DOA) State Security Office (SSO) for approval. The process for certification for production is based on the Authorization Package approval and application testing of the security controls. After a successful security test process is complete the system would be ready for acceptance and production based on security requirements. This may require changes and updates to the system by the Offeror. The Offeror must plan activities to support security control verification and an appropriate number of remediation iterations to address defects identified.

3.7.2.3 Requirement – Business Associate Agreement

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

3.7.2.4 Requirement – Authority to Operate

Once all security compliance is established via approved system Authorization Packages(s) and signed Business Associate Agreements (BAA) or data usage agreements, as applicable, the solution will be granted an Authority to Operate (ATO) by the OIT Department Technology Officer for DHSS and the DHSS designated Division Data Owner. Phased projects must obtain the ATO for each phase completion resulting in a production change. The Offeror must plan activities and milestones that support obtaining the ATO prior to production rollout. The Offeror's plan must include schedule contingencies to mitigate DHSS business risks of failing to obtain the ATO by the business deadlines. For example, if the DHSS organization using the solution must have the solution operating by December 1st, the Offeror's plan must include schedule contingencies and mitigations to ensure the ATO is received well ahead of December 1st with enough time for the DHSS organization to communicate with stakeholders if that deadline is at risk of being met.

3.7.3 Auditing and Logging Integration

All systems are required to be capable of generating data access and recording by user id requesting, or reading and writing of data.

For logging and audit, DHSS uses SPLUNK. All systems are required to be capable of generating data access and recording by user id requesting, or reading and writing of data. The application must be readily capable of generating logging and auditing in a concise summary that can be easily integrated into SPLUNK. 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.

The application must be readily capable of generating logging and auditing in a concise summary that can be easily integrated into SPLUNK. The package produced by the application must be inclusive of all the data for who is accessing, reading, and writing the data.

3.7.3.1 Requirement

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

3.7.4 Data Security

The Department of DHSS is considered a single covered entity in regards to HIPAA and APIPA which governs security requirements for ePHI, HIPAA, and PII. DHSS owns the data and can demand it at any time. Proposed solutions that leverage public or private data sources resulting in DHSS business decisions – especially where the business decision reflects a DHSS legal jurisdiction related to due process – must ensure DHSS retains access to all the data required to support the decision.

3.7.4.1 Requirement

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

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.

3.7.4.2 Requirement – Recovery Point and Recovery Time Objectives

The Offeror's proposed solution must include and define RPO and RTO capabilities.

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 DHSS operating environment, and ensure that many of the required controls are met at the least cost, DHSS has implemented an Enterprise Service Bus (ESB) and partnered with the heatheConnect 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-DHSS premise and Off-site hosted information systems.

3.7.5.1 Requirement

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

~~3.7.6 DHSS Managed Off-site Hosting Considerations~~

This section intentionally removed.

~~*3.7.6.1 Requirement*~~

This section intentionally removed.

~~*3.7.6.2 Requirement*~~

This section intentionally removed.

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

Software as a Service (SaaS) and Anything as a Service (XaaS) delivery models afford DHSS the ability to leverage the business value of information management solutions without bearing the costs and risks of having to maintain development and operational infrastructure. This value is achieved when the SaaS 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.

DHSS IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DHSS IT Information Security Compliance and Privacy Services and Standards. Specifically, when federal funding rights do not apply, and when DHSS 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 DHSS 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 DHSS Archer 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.

SaaS/XaaS offerings must have a FISMA network vulnerability scan performed at least once every 30 days, with the results provided to the Department Security Office (DSO) and the Division Data Owner. SaaS offerings must have an automated code scan, or manual analysis of code security, performed at least once every 90 days, with the results provided to the Department Security Office and the Division Data Owner.

At time of contract, the Offeror must provide responses to IT Reference H and sign the **Error! Reference source not found.** HIPAA Business Associate Agreement (located in the Standard Agreement Form attached to the solicitation) or data usage agreement. During the development activity the Offeror, in conjunction with DHSS, must complete answers to a DHSS RSA Archer Authorization Package.

3.7.7.1 Requirement – SaaS/XaaS Security Responsibilities

Proposals for SaaS/XaaS offerings should include confirmation the Offeror will be responsible for all security mechanisms within their environment. Including encrypting and securing any HIPAA data, and will adopt the latest security measures available to prevent unauthorized access.

The Offeror is also responsible for server patching and completing an RSA Archer Authorization Package. The Offeror must assume the responsibility for all authentication and account creations or modifications.

3.7.7.2 Requirement – SaaS/XaaS Logging and Auditing

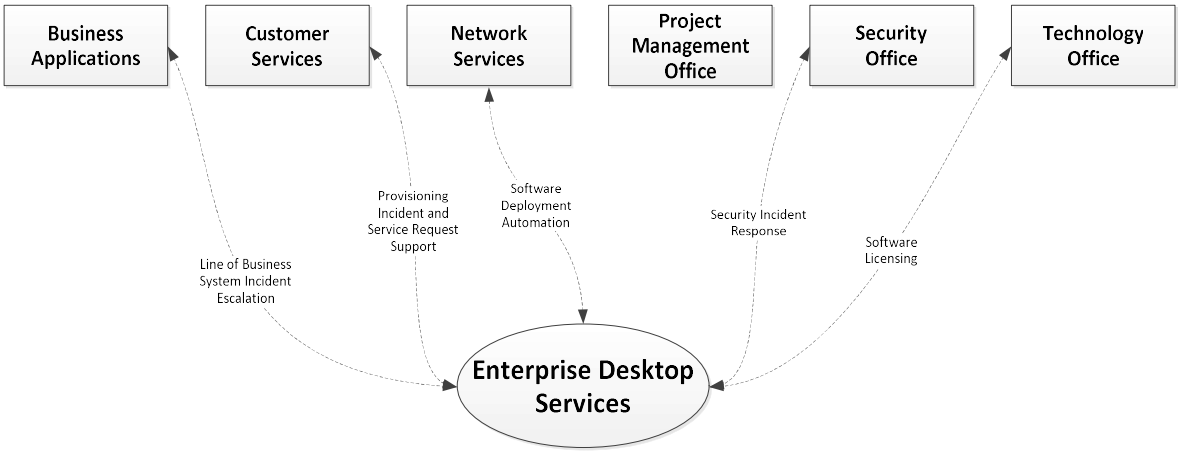
For proposals that include SaaS/XaaS solutions that may manage confidential data, the SaaS/XaaS must include a logging and auditing solution. All components and systems within the Offeror's proposal are required to be capable of generating data access and recording by user id requesting, or reading and writing of data. 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 provide responsible DHSS entities (DSO, Division Data Owner) access to perform oversight related tasks. The package 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.

3.8 Enterprise Desktop and Mobility Services and Standards

Enterprise Desktop and Mobility Services include the activities DHSS ITS performs to define, deploy and support the DHSS enterprise desktop and mobility endpoints. DHSS 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 DHSS end-user desktops.

Enterprise Desktop and Mobility Services is matrixed per the following organizational mapping:



3.8.1 Desktop Access and Configuration

DHSS is a Dell Hardware shop so all workstations are Dell. Offerors should propose solutions that are device independent. The DHSS Enterprise Desktop is a support 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).

DHSS is a least privilege environment and staff do are not granted elevated privilege without individual, reviewed and approved security policy waivers. DHSS Program staff work with DHSS ITS to request, review and determine compatibility, redundancy and fit of new, non-standard software. DHSS Program staff are not permitted, and cannot independently authorize, or install, new software components, or applications, on the desktop. Offerors should avoid solutions that require customization of the DHSS Enterprise Desktop.

If the Offeror's proposed solution requires use of a desktop web browser, the solution should be browser independent and be fully capable of functioning with the standard browser in the DHSS 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 DHSS 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 DHSS 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 DHSS Enterprise Desktop. The Offeror must include activities in their proposal to work with the DHSS Enterprise Desktop team to integrate each non-standard software component. These activities must include working with DHSS 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 DHSS currently deployed web browser version(s). The required functionality of the solicitation 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 DHSS standard browser vendor's published support lifecycle material published at the time of proposal and include in their proposal a plan to upgrade off of any versions of browser that are known to become unsupported during the execution of the contract. The Offeror must include in their cost proposal the optional contingency cost of one unanticipated browser compatibility version upgrade for the components of the proposed solution where they own the code or are responsible for maintaining it.

3.8.1.3 Requirement – Desktop Productivity Software Compatibility

The Offeror must include in their cost proposal the optional contingency cost of one unanticipated browser compatibility version upgrade for the components of the proposed solution where they own the code or are responsible for maintaining it. The Offeror must plan to support DHSS currently deployed desktop productivity suite version(s). The Offeror must review the DHSS standard desktop productivity suite vendor's lifecycle material published at the time of proposal and include in their proposal a plan to upgrade off of an versions of productivity suite software identified as becoming unsupported during the planned execution of the contract. 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 DHSS are:

- Dell 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, Google Chrome.

    - Software should not be dependent on a specific version of MS Office Suite. We are currently at 2013 – but we move the organization as a whole for the Department upgrades. DHSS has over 4000 Department Staff.
- Apple IOS 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 are currently at 2010 – but we move the organization as a whole for the Department upgrades. We have over 4000 Department Staff.

Dell and Apple Devices are configured with the latest operating systems or 1 version previous. The DHSS mobile device strategy is evolving rapidly and is not stable or complete for supporting the ability to store or transmit confidential data. Offerors should plan extensive engagement with the DHSS Enterprise Desktop and Mobility service line if their solution includes mobile device end-points.

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 DHSS 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 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.8.3.1 Requirement*~~

This section intentionally removed.

~~*3.8.3.2 Requirement*~~

This section intentionally removed.

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

This section intentionally removed.

~~*3.8.4.1 Requirement*~~

This section intentionally removed.

~~3.9 DHSS Hosting and Datacenter Services and Standards~~

This section intentionally removed.

~~3.9.1 On-DHSS Premise Hosting Considerations~~

This section intentionally removed.

~~*3.9.1.1 Infrastructure*~~

This section intentionally removed.

~~*3.9.1.2 Platform*~~

This section intentionally removed.

~~*3.9.1.3 Requirement*~~

This section intentionally removed.

~~*3.9.1.4 Requirement*~~

This section intentionally removed.

~~3.9.2 DHSS Managed Off-site hosting considerations~~

This section intentionally removed.

~~*3.9.2.1 Requirement*~~

This section intentionally removed.

~~*3.9.2.2 Requirement*~~

This section intentionally removed.

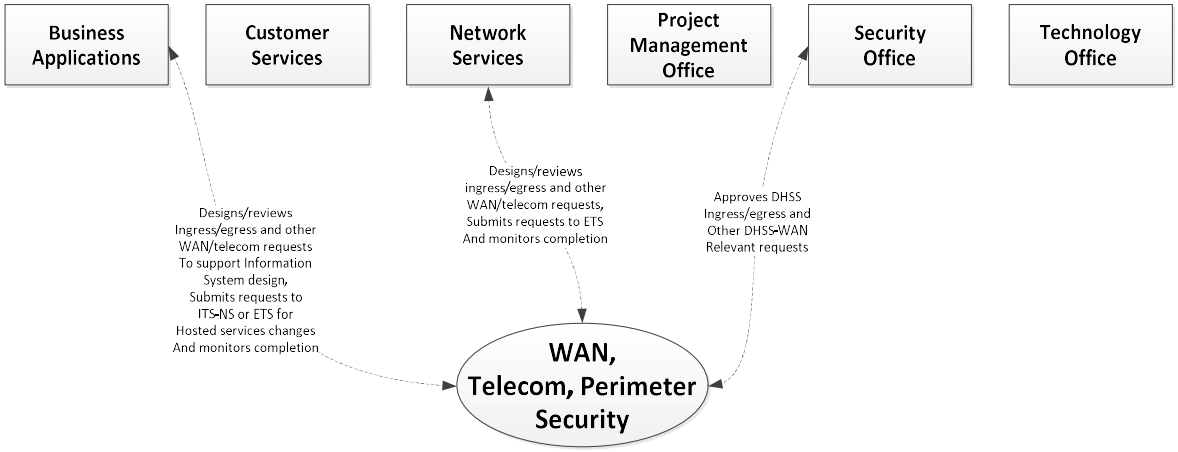
~~3.9.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios~~

This section intentionally removed.

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

DHSS Wide Area Network, Telecommunications and Perimeter Security Services include the activities DHSS IT performs to integrate the DHSS 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, DHSS 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 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, currently Service Desk Manager (SDM).

DHSS Wide Area Network, Telecommunications, and Perimeter Services is matrixed per the following organizational mapping:



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 DHSS 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.

~~3.10.2 DHSS Managed Off-site Hosting Scenarios~~

This section intentionally removed.

~~*3.10.2.1 Requirement*~~

This section intentionally removed.

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

This section intentionally removed.

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.). DHSS 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

DHSS requires ADA compliant application access. Many people with disabilities use "assistive technology" to enable them to use computers and access the Internet. Blind people who cannot see computer monitors may use screen readers – devices that speak the text that would normally appear on a monitor. People who have difficulty using a computer mouse can use voice recognition software to control their computers with verbal commands.

Poorly designed websites can create unnecessary barriers for people with disabilities, just as poorly designed buildings prevent some from entering. Designers may not realize how simple features built into a web page will assist someone who, for instance, applications must work with screen readers for people who cannot see a computer monitor or use a mouse.

When accessible features are built into web pages, websites are more convenient and more available to everyone – including users with disabilities. Web designers can follow techniques developed by private and government organizations to make even complex web pages usable by everyone including people with disabilities. For most websites, implementing accessibility features is not difficult and will seldom change the layout or appearance of web pages. These techniques also make web pages more usable both by people using older computers and by people using the latest technologies (such as personal digital assistants, handheld computers, or web-enabled cellular phones).

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 and has a useful guide for web developers at www.access-board.gov/sec508/guide/1194.22.htm ;

The Department of Justice also has information about accessible web page design in an April 2000 report to the President. This report is available at www.usdoj.gov/crt/508/report/content.htm, and the General Services Administration hosts an online course for web developers interested in accessible web design. This program was developed in conjunction with the Access Board, the Department of Justice, and the Department of Education and provides an interactive demonstration of how to build accessible web pages. This course is available at www.section508.gov, which also provides information about the Federal government's initiative to make its electronic and information technology accessible to people with disabilities.

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 www.w3c.org/WAI/Resources, and Information about the Web Accessibility Initiative can be found at www.w3c.org/WAI .

3.11.1.1 Requirement

DHSS 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 accessible by American's with Disabilities.

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

It is **critical** that the Offeror understand that the State of Alaska Department of Health and Social Services (DHSS) is evolving from a traditional model of program-centric administration based on division-level technology needs, to a Department-level, enterprise-wide architecture based on the leveraging of shared technology and business components. The result for DHSS is a modular, flexible Health Information Technology (HIT) architecture, designed to allow the Department to meet current and future business needs, with a focus on lower cost, increased efficiency, and improved service.

The result for Alaska is the transition from a Division-centric IT approach to one that aligns with the technical and business needs across the Department, supporting the implementation and sharing of common components across Divisions. The full implementation of the Department IT Technology Standards establishes the following guiding principles and strategies:

- Maximize use of DHSS HIT expenditures through reuse of shared technology and business services, allowing functionality and services to be exposed for reuse
- Alignment of business needs and business processes across Divisions
- Migration to a DHSS-enterprise, consumer-centric focus, moving away from siloed, program-specific perspectives.

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

3.12.2 Modularity

This condition requires the use of a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (API); the separation of business rules from core programming; and the availability of business rules in both human and machine readable formats. This is in order to ensure that states can more easily change and maintain systems, as well as integrate and interoperate with a clinical and administrative network designed to deliver person-centric services and benefits.

3.12.3 MITA Condition

This condition requires states to align to and advance increasingly in MITA maturity for business, architecture, and data. State are to complete and continue to make measurable progress in implementing their MITA Maturity Model roadmaps, MITA State Self-Assessments, and Concept of Operations (COO) and Business Process Models (BPM).

This requirement requires a demonstration of understanding of the CMS Seven (7) Standards and Conditions and the Department's IT Technology Standards (See IT Reference D) and how this applies to the Contractor's proposed solution.

3.12.4 Industry Standards Condition

States must ensure alignment with, and incorporation of, industry standards: the Health Insurance Portability and Accountability Act (HIPAA) of 1996 security, privacy and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with federal civil rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act (ACA); and standards and protocols adopted by the Secretary under section 1561 of the ACA.

3.12.5 Leverage Condition

State solutions should promote sharing, leverage, and reuse of Medicaid technologies and systems within and among states. This condition encourages states to identify any components and solutions that are being developed with the participation of or contribution by other states; solutions that have high applicability for other reuse by other states; and service-based and cloud-first strategy for system development.

3.12.6 Business Results Condition

Systems should support accurate and timely processing of claims (including claims of eligibility), adjudication, and effective communications with providers beneficiaries, and the public. A system should employ effective and efficient business process, producing and communicating the intended operational results with a high degree of reliability and accuracy.

3.12.7 Reporting Condition

Solutions should produce transaction data, reports, and performance information that contribute to program evaluations, continuous improvement in business operations, transparency, and accountability

3.12.8 Interoperability Condition

Systems must ensure seamless coordination and integration with health insurance exchanges (whether run by the state or federal government), and allow interoperability with health information exchanges, public health agencies, human service programs, and community organizations providing outreach and enrollment assistance services.