REQUEST FOR PROPOSALS ("RFP")

Date Issued: May 2, 2024

The Ohio Department of Higher Education ("ODHE") is requesting proposals for:

Online Apprenticeship Management Software System

Signed proposals must be submitted via email to edapprentice@highered.ohio.gov by 5:00 PM EST on May 16, 2024.

Estimated Schedule

RFP Release: May 2, 2024

Questions due by: May 8, 2024

Responses to questions received by the deadline: May 10, 2024

Proposal Submission Deadline: May 16, 2024 by 5:00 p.m. Est

Anticipated Award Date: On or before May 22, 2024

I. Background

The Ohio Departments of Higher Education, Education, and Jobs and Family Services partnered together to develop the standards of the program now recognized by the State Apprenticeship Agency. The Ohio Departments of Higher Education and Jobs and Family Services will coordinate to approve apprenticeships with the Ohio Department of Higher Education serving as the sponsor and the Ohio Department of Jobs and Family Services approving apprentices sponsored by the ODHE.

Current guidelines and procedures for submitting apprenticeship programs can be found on the ODHE website here: https://highered.ohio.gov/educators/academic-programs-policies/academic-program-approval/educator-preparation/ed-apprenticeship

II. Scope of Work:

The Ohio Department of Higher Education requests proposals for a state-level apprenticeship management software system.

1. **Submission Platform**: Implement a system allowing state staff, apprentice participating districts, higher education institutions, and partners to electronically submit applications, appendices, and other apprenticeship program documents to the Ohio Department of Higher Education ("ODHE").
2. **Tracking and Reporting**: Develop capabilities to track, filter, and generate reports on individuals involved in the apprenticeship program from application to completion.
3. The related instruction provider should have the ability to document an apprentice's progress and track the apprentice's progress at the end of each term to determine if the apprentice has satisfactorily fulfilled the course requirements. This information should be accessible to all necessary parties as instructed by ODHE for comprehensive oversight of all progress.
4. The mentor/teacher should possess the ability to assess the apprentice's advancement based on the Ohio Standards for the Teaching Profession by assigning tasks and assignments for completion. Additionally, the application should enable the apprentice to upload documents as evidence of task completion.
5. The application should be able to fulfill the RAPIDS 671 requirements form.
6. The system should have the capacity to store applications, sponsorship intents, and employer acceptance agreements securely for a period of five years.
7. Ensure that the Ohio Standards of the Teaching Profession evaluation dashboard is embedded appropriately into the application.
8. **Responsibilities and access capabilities:**
    a. The State Manager will possess full access to the entire dashboard, enabling them to view and make changes as needed.
    b. Signatory Employer manager should be able to monitor the progress of all apprentices they employ.
    c. Mentors/Teachers will access their apprentices' information and be able to manage, and add tasks, and activities for them, including the evaluation.
    d. Apprentices will have access limited to their view, enabling them to monitor their progress throughout the program and access their assigned tasks and activities, upload documents, and even suggest, and create activities to meet requirements.
    e. The application has the ability to assign tasks within the organization.

9. **Reporting and Monitoring Features in Apprenticeship Management Platform**
    a. Real-time reporting is available directly from the platform.
    b. Customizable report settings to tailor data analysis.
    c. An alert system to notify all levels of managers of apprentice progress, including RTI and OJT task completion.
    d. Comprehensive progress and performance dashboards for monitoring apprentice development.
10. **Email Notifications**: Incorporate email notification functionality to inform stakeholders of actions taken on proposals, progress report prompts, and upcoming deadlines, ensuring timely communication throughout the process.
11. **Comprehensive Database**: Create a centralized database within the system to maintain a comprehensive list of individuals at any phase of an apprenticeship program in Ohio, providing easy access to program-related information.
12. **Authoritative Source**: Establish the system as the authoritative source for all apprenticeship programs submitted and approved by ODHE, ensuring data accuracy and integrity.
13. **Data Exchange Mechanism**: Implement a web service or similar mechanism to facilitate the exchange of data between the system and relevant stakeholders, enabling seamless information sharing and updates.
14. The application would include functionality to aggregate and disaggregate apprentice demographics at both statewide and regional levels. This feature enables the creation of detailed reports on the apprentices within the program. Additionally, the database will store demographic data securely to facilitate accurate reporting and analysis.

Responders to the RFP should have a software system, solution or platform that has previously been developed and implemented at a statewide or regional level. The company should have evidence of success in developing and implementing a management program, apprenticeship workflow systems and databases at the state and regional levels. Extensive knowledge of apprenticeship program issues at the state level is required.

Please indicate your company's ability to accomplish the items above with the estimated implementation date for each item.

III. Cost

The Offeror must provide the cost of the implementation of the online system including training.

The Offeror must provide costs for maintenance and specify the frequency of such costs.

IV. Training

The Offeror shall train ODHE staff in the operation of the system and software within thirty (30) days of delivery with approved appointment dates. A training manual should also be provided.

V. References

The Offeror must provide three (3) references from previous clients using a similar system during the past five (5) years.

VI. State of Ohio IT Requirements

1) Supplement A - The Offeror must complete the attached Supplement A and submit it with the Proposal.
2) State of Ohio Data Security and Privacy Terms – Offeror understands that by submitting a proposal in response to this RFP, they are agreeing to comply with the State of Ohio Data Security and Privacy Terms attached hereto.

VII. General Instructions for Proposal Submittal

Each Offeror must submit a scope of work, cost outline, training, evidence of experience with similar software, and extensive knowledge of apprenticeship program issues, as well as the completed Supplement A, as part of its total Proposal on or before due date. Proposal documents may be submitted via email as Microsoft Office documents (e.g., Word or Excel) or as PDF documents via email or submitted through a website.

Proposals are due no later than 5:00 PM EST on May 16, 2024. Offers must submit Proposals to edapprentice@highered.ohio.gov.

VIII. Legal Notices

The Offeror understands that if its proposal is accepted by the ODHE, the Offeror shall enter into an agreement with ODHE governing the use of the awarded funds. The Offeror agrees to comply with all applicable federal, state, and local laws and regulations in the conduct of the work hereunder.

ODHE reserves the right to fund any proposal in full or in part, to request additional information to assist in the review process, to require new proposals from interested parties, to reject any or all proposals responding to this announcement, or to reissue the announcement if it is determined that it is in the best interest of the State of Ohio. Issuing this announcement does not bind ODHE to making any awards. ODHE reserves the right to adjust the dates for this announcement for whatever reasons are deemed appropriate. ODHE reserves the right to waive any non-substantive infractions made by an Offeror, provided that the Offeror cures such infraction upon request.

All costs incurred in preparation of a proposal shall be borne by the Offeror. Proposal preparation costs are not recoverable under an award. ODHE shall not contribute in any way to recovering the costs of proposal preparation.

The funding decisions are final. Offerors will be notified of the outcome of their proposal(s) at the conclusion of the review process.

The Offeror understands that the information provided herein is intended solely to assist the Offeror in submittal preparation. To the best of ODHE's knowledge, the information provided is accurate. However, ODHE does not warrant such accuracy, and any errors or omissions subsequently determined will not be construed as a basis for invalidating this solicitation. Interested parties bear the sole responsibility of obtaining the necessary information to submit a qualifying proposal. ODHE retains the right to modify or withdraw this solicitation at any time. By submitting a proposal, Offerors expressly agree to these terms.

IX. Trade Secrets

All Offerors are strongly discouraged from including in a proposal any information that the Offeror considers to be a "trade secret," as that term is defined in Section 1333.61(D) of the Ohio Revised Code.

1. To determine what qualifies as trade secret information, refer to the definition of "trade secret" in the Ohio Revised Code at 1333.61(D), which is reproduced below for reference:

   "(D) 'Trade Secret' means information, including the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, pattern, compilation, program, device, method, technique or improvement, or any business information or plans, financial information, or listing of names, addresses, or telephone numbers that satisfies both of the following:

   (1) It derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

   (2) It is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

2. If any information in the proposal is to be treated as a trade secret, the proposal must:

   a. Identify each and every occurrence of the information within the proposal with an asterisk before and after each line containing trade secret information and underline the trade secret information itself;

   b. Identify that the proposal contains trade secret information in the cover letter; and

   c. Include a summary page immediately after the cover letter that lists each page in the proposal that includes trade secret information and the number of occurrences of trade secret information on that page.

3. The Ohio Department of Higher Education requires non-disclosure agreements from all non-Department of Higher Education persons who may have access to proposals containing trade secret information, including evaluators.

4. If the Offeror claims that a record is not subject to disclosure under the Ohio Public Records law based on trade secret, it will bear costs of defending this claim.

Supplement A:

State IT Policy, Standard and Service Requirements

Revision History:

Date:	Description of Change:
1/01/2019	Original Version
10/18/2019	Updated to modify service descriptions, include new services, and remove older services. A new Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements was added.
12/15/2020	Updated to align with current service offerings, to incorporate the Cloud Smart strategy, and to clarify the variance request requirements.
5/13/2021	Updated to align with current Infrastructure as a Service (IaaS) Frameworks service offering.
7/19/2021	Updated to modify service descriptions, include new services, and remove older services.
02/07/2022	Updated Section 4.1. State IT Cloud Smart Strategy to clarify the scope, intent, and requirements of the service. Also, reorganized the public and private cloud information.
05/03/2022	Updated Section 4.3.6 ePayment Business Solutions audit standard. Modified Section 3. State IT Policy and Standard Requirements to remove the references to State of Ohio IT Bulletins and revise hyperlinks.

Contents

1. Overview of Supplement and Requirements

This supplement shall apply to any and all work, services, locations and computing elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State of Ohio ("State") and any access to State resources in conjunction with delivery of work.

This includes, but is not limited to:

- Major and minor projects, upgrades, updates, fixes, patches and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized change orders, change requests, statements of work, extensions or amendments to this contract;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-contracted personnel that have access to State Data as defined below:
    - "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.
    - "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. Sensitive Data includes but is not limited to:
        - Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.
        - Federal Tax Information (FTI) under IRS Special Publication 1075.
        - Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).
        - Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.
        - The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.
- The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in the Contract shall prevail.

Contractors performing the work under the Contract are required to comply with Ohio and the Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) ("DAS OIT") policies and standards (refer to Section 3 for additional information) and leverage State IT services outlined in this document unless the State has approved a variance. Refer to Section 2 for instructions on proposing variances to the requirements outlined in this supplement.

2. Proposed Variances to Supplement Requirements

ANY PROPOSED VARIANCES TO THE REQUIREMENTS OUTLINED IN THIS SUPPLEMENT ARE REQUIRED TO BE IDENTIFIED IN APPENDIX A - REQUEST FOR VARIANCE TO STATE IT POLICY, STANDARD OR SERVICE REQUIREMENTS. OFFERORS ARE ASKED NOT TO MAKE ANY CHANGES TO THE LANGUAGE CONTAINED WITHIN THIS SUPPLEMENT. In the event the Offeror finds it necessary to deviate from any of the IT policies, standards or State IT services, a variance may be requested, and the Offeror must provide a sufficient business justification for the variance request. In the event that a variance is requested post award (e.g., a material change to the architecture), the Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

3. State IT Policy and Standard Requirements

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.

Table 1 – State of Ohio and DAS IT Policies and Standards

Item	Link
State of Ohio IT Policies	https://das.ohio.gov/technology-and-strategy/policies
State of Ohio IT Standards	https://das.ohio.gov/technology-and-strategy/policies
DAS Policies	100-11 Protecting Privacy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series https://das.ohio.gov/technology-and-strategy/policies

Please affirm compliance with the State's IT policies and standards. If this section, or portions of this section are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4. State of Ohio IT Services

DAS OIT delivers information technology (IT) and telecommunication services. DAS OIT is responsible for operating and maintaining IT and telecommunication hardware devices, as well as the related software. The supplement outlines a range of service offerings from DAS OIT that enhance performance capacity and improve operational efficiency. Explanations of each service are provided and are grouped according to the following solution categories. Where applicable, Contractors are required and expected to incorporate these services into their solutions or provided services.

4.1. State IT Cloud Smart Strategy

Executive Order 2019-15D, "Modernizing Information Technology Systems in State Agencies," required all cabinet agencies, boards and commissions to migrate information technology systems to the State's cloud environment managed by DAS OIT. From this executive order, the State IT Cloud Smart Strategy ("Strategy") evolved to support agency cloud service needs. The Strategy is designed to provide a value-driven, dynamic, and cost-effective set of differentiating core enterprise services and innovative technologies from public and private clouds that will improve State of Ohio operations and the quality of services to Ohioans.

As part of the Strategy, DAS OIT will operate a Cloud Center of Excellence ("CCoE") to focus on leveraging the State's investment in the private cloud, while incorporating efficiencies from public cloud providers. The CCoE provides guidance that will assist in realizing the value of a multi-cloud investment. The goal is to evaluate and provide the most optimal hosting environment in the State's public and/or private clouds. The CCoE offers an Enterprise Cloud Brokerage Service ("Brokerage Service") that supports and guides State Agencies ("Agencies") as they look to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) application and solution modernization opportunities.

The Strategy requires any proposed customized applications[1] running on an IaaS or PaaS public cloud to reside in the Brokerage Service (Microsoft Azure, Amazon Web Services, Oracle Cloud Infrastructure, Google Cloud Platform or IBM Cloud). Applications developed and hosted in low code or no code platforms (e.g., Salesforce, Power Apps, or ServiceNow) will not reside within the Brokerage Service and will be addressed on a case-by-case basis.

Any proposed statewide or individual Agency solution must comply with the Strategy.

[1] **Customized Applications**: In terms of this Supplement, this term refers to applications that are specifically written, modified, or adapted for the State of Ohio.

(**Please Note**: If the Offeror feels that these requirements cannot be accommodated, an explanation **must be provided** at the end of this section **and a proposed variance** needs to be defined in Appendix A.)

4.1.1. Public Cloud Brokerage Service

DAS OIT is leading the effort to transform how IT services are delivered, maintained, and consumed in the State of Ohio. A key outcome of this digital transformation is the development of cloud-based capabilities that will improve the quality of services, agility, and foster a culture of collaboration, accountability, and innovation.

This service is available on multiple public clouds: Microsoft Azure, Amazon Web Services, Oracle Cloud Infrastructure, Google Cloud Platform and IBM Cloud.

Within the Public Cloud Brokerage Service model, DAS OIT offers IaaS, PaaS, and vendor managed frameworks. These service offerings are described in detail in the sections below.

4.1.1.1. IaaS Cloud Brokerage Service

The IaaS Cloud Brokerage Service is a DAS OIT managed service similar to the Private Cloud Data Center. DAS OIT will architect, configure and run all IaaS implementations, whether on premises or in a public cloud. The same tools are used to update, secure, and manage the virtual machines, no matter the location (private or public cloud).

Within the established framework for each public cloud, the customer has read access to their infrastructure running in a specific public cloud. The customer cannot create or manage compute items without receiving an approved exemption due to Executive Order 2019-15D referenced above. While customers cannot create any network peering, they can request peering back to the State Private Cloud via dedicated private connections.

IaaS Cloud Brokerage Service offers:

- Configuring network security groups and backups
- Performing restores
- Storage
- Providing a direct network connection to the State of Ohio Computer Center from public cloud vendor locations
- Managing and monitoring using the same tools as the Private Cloud
- Patching
- Design consultation
- Education
- Offering specific cloud expertise, when needed

4.1.1.2. PaaS Cloud Brokerage Service

The PaaS Cloud Brokerage Service offers customers the ability to request an environment in one of the State's public clouds. The PaaS environment allows the customer to consume the appropriate cloud native services.

Within the established framework for each public cloud, the customer can create and manage available PaaS cloud offerings.

PaaS Cloud Brokerage Service offers:

- Vendor management
- Providing the initial framework for build and configuration
- Service provisioning, implementation, monitoring and alerting
- Role-Based Access Control Security
- Enforcing Base Compliance Policies
- Active directory account integration, when appropriate
- Assistance in service request resolution via the native cloud portal and the DAS OIT Customer Service Center
- Design consultation
- Education

- Offering specific cloud expertise, when needed

4.1.1.3. Vendor Managed Cloud Brokerage Service

The Vendor Managed Cloud Brokerage Service is a vendor-managed application infrastructure within the State's public cloud framework pursuant to a contract entered into between a customer and the managing vendor.

Operating within this environment helps to ensure that the State's data remains in the U.S., the initial build and configuration is within the State's framework and overlap is avoided in the IP (Internet Protocol) space through network addressing standards.

In terms of the Vendor Managed Cloud Brokerage Service, the Brokerage Service is responsible for:

- Vendor management
- Providing the initial framework for build and configuration
- Role-Based Access Control Security
- Design consultation
- Education
- Offering specific cloud expertise, when needed

If the proposed solution cannot accommodate the State's Strategy and CCoE requirements listed above, please provide a justification for the exception in the space below. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the Supplement shall not be modified.

4.1.2. Private Cloud Data Center Services

4.1.2.1. AIX Systems

Advanced Interactive Executive (AIX) is a proprietary version of the UNIX operating system developed by IBM. The AIX Systems Service enables customers to develop and run applications and/or databases without incurring the cost of setting up, administering and maintaining an operating system environment. DAS OIT runs the AIX operating system on IBM Power hardware, as a physical server or logical partition (LPAR)/virtual server. All of the AIX systems are connected to the DAS OIT Enterprise Storage Area Network (SAN) for performance, general purpose or capacity based storage. All systems are also provided backup and recovery services.

4.1.2.2. Enterprise Backup Services

The Enterprise Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available for customer data. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

4.1.2.3. Data Center Co-Location Service

The DAS OIT Co-Location service offers customers a Tier 3 capable secure data center environment with reliable uptime, power redundancy and redundant cooling to ensure uninterrupted access of critical data and applications in the State of Ohio Computer Center (SOCC). The SOCC is staffed and available to authorized personnel 24 x 7 x 365 and is accessible via electronic card key only.

4.1.2.4. Enterprise Data Storage

DAS OIT will work with the Contractor and customer to determine the optimal data storage solution, if applicable. The services covered under Enterprise Data Storage include:

High Performance Disk Storage service offers high-performance, high-capacity, secure storage designed to deliver the highest levels of performance, flexibility, scalability and resiliency. The service has fully redundant storage subsystems, with greater than five-nines availability, supporting mission critical, customer-facing and revenue-generating applications 24x7x365. High Performance Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

General Purpose Disk Storage service offers a lower-cost storage subsystem for customers not requiring high performance disk. This service supports a wide range of applications, including email, databases and file systems. General Purpose Disk is also flexible and scalable and highly available. General Purpose Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

Capacity Disk Storage service is the least expensive level of disk storage available from DAS OIT. Capacity Disk is suitable for large capacity, low performance data, such as test, development and archival. Capacity Disk Storage is supplied as dual Enterprise SAN fiber attached block storage or as file based storage.

4.1.2.5. Open Systems DR-DRaaS

Open Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus, Ohio. The service provides customers with a private Disaster Recovery as a Service solution connected to the SOCC via the Ohio One Network that will consists of the following:

- Compute to allow expected performance in the event of a complete failover
- 24vCPU per host with 32 host in the environment all licensed with VMware
- Support of the orchestration and replication environment
- Site connectivity
- Stored images available upon demand

Open Systems Disaster Recovery - Windows (1330 / 100607 / DAS505170/ 3854L) - Open Systems Disaster Recovery – Windows is a service that provides a secondary failover site for Windows based servers within the geographically disparate site. This service provides duplicative server compute and storage to match Server Virtualization and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

Open Systems Disaster Recovery - AIX (1330 / 100607 / DAS505170/ 3854N) - Open Systems Disaster Recovery – AIX is a service that provides a secondary failover site for AIX based servers within the geographically disparate site. This service provides duplicative server compute and storage to match AIX Systems Services and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

4.1.2.6. Mainframe Business Continuity and Disaster Recovery

Business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery, a subset of business continuity focuses on restoring the information technology systems that support the business functions.

Mainframe Disaster Recovery (DR) services are offered to customers of DAS OIT's IBM mainframe environment. Services are made available via IBM's Business Continuity and Resiliency Services which provides hot site computer facilities at a remote location.

Tests are conducted annually at IBM's hot site location, during which DAS OIT's mainframe computer infrastructure is restored. Once the mainframe system is operational, participating Agencies restore their production applications and conduct extensive tests to ensure that those applications have been successfully recovered and would be available in the event of an actual disaster.

This service is designed to expand business continuity and disaster recovery capabilities in the most cost effective and efficient manner possible for DAS customers and for Agencies that have systems and applications that run on DAS/OIT infrastructure at the SOCC.

4.1.2.7. Mainframe Systems

DAS OIT's Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5052 Million of Instructions per Second (MIPS). This mainframe uses the z/OS operating system and the Job Entry Subsystem (JES3). Additionally, the system is connected via fiber to DAS OIT's High Performance Disk Storage, which affords reliable and fast disk access and additional storage capacity when needed.

Services are provided using a wide range of application, transaction processing and telecommunications software. Data security and user authentication are provided by security software packages. This service enables customers to develop applications without incurring the costs of setting up and maintaining a mainframe operating system environment.

Mainframe tape service option is available:

- Mainframe Virtual Tape - Virtual tape technology that optimizes batch processing and allows for better tape utilization using the EMC Disk Library for Mainframe (DLM) virtual tape.

4.1.2.8. Metro Site Facility

The Metro Site Facility Service provides a secondary, near real-time (measured in milliseconds) failover from the SOCC. This service provides for the facility, site connectivity, on-going support of server images for Disaster Recovery as a Service, and associated services. Metro Site Facilities are offered to support Virtual Server and Data Storage customers providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area. This service provides duplicative server facilities to match Server Virtualization and Data Storage Rates. Storage necessary for support of the disaster recovery image will be billable at the standard storage rates.

4.1.2.9. Server Virtualization

Server Virtualization is the practice of abstracting the physical hardware resources of compute, storage and networking of a host server and presenting those resources individually to multiple guest virtual servers contained in separate virtual environments. DAS OIT leverages the VMware vSphere platform to transform standardized hardware into this shared resource model that is capable of providing solutions around availability, security and automation.

Server Virtualization includes:

- **OIT Managed-Basic Server Virtualization**: DAS OIT hosts the virtual server and manages the hardware/virtualization layer. DAS OIT is also responsible for managing the server's operating system (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of General Disk Storage used for the operating system.

If the proposed solution cannot accommodate the State's Private Cloud Data Center Services listed above, please provide a justification for the exception in the space below. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.2. InnovateOhio Platform

Executive Order 2019-15D, "Modernizing Information Technology Systems in State Agencies," established the InnovateOhio Platform (IOP) initiative. IOP focuses on digital identity, the experience of the individual authorized to access the system ("User"), analytics and data sharing capabilities. The InnovateOhio Platform provides integrated and scalable capabilities that better serve Ohioans.

4.2.1. Digital Identity Products

OH | ID - Digital identity solution for Ohio citizens:
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for citizens. Multiple levels of identity assurance.

- Single Sign-On
- Access Logging
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Access Management
- Self-Service Portal
- Identity Proofing
- Directory Integration

OH | ID Workforce - Digital identity solution for Ohio workforce
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for state and county employees, contractors, and external workers. Multiple levels of identity assurance.

- Single Sign-On
- Directory Integration
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Just-in-Time Provisioning
- User Management
- Access Logging
- Privileged Access Management

ID Platform – Software as a Service (SaaS) identity framework
Provides authorization layer for use by Agencies and programs. Allows Agencies to integrate and extend InnovateOhio Platform identity services into their applications. Customizable to Agency needs.

- Fine-Grain Authorization Management
- Real-Time Analytics
- Extendable Services from OH|ID
- Cloud-Based Infrastructure

4.2.2. User Experience Products

IOP Portal Builder - Website template accelerator:
An accelerator to easily create modern, responsive, and ADA-compliant websites and portals for the InnovateOhio cloud platform. The InnovateOhio Portal Builder is available in a Software as a Service (SaaS) form.

- Standardized Dynamic Templates
- Automated Workflows
- Governance & Access Control
- Optimized Content Search
- ADA-Compliant
- Content Management
- Integration with OH|ID
- Real-Time Analytics
- Aggregate Applications
- Customizable Features
- Mobile Ready
- Site Analytics

IOP myOhio - The State's Intranet platform
Features intuitive navigation, simplified access to on-boarded business applications, and a modernized, mobile-responsive design. Automates compliance with accessibility standards per Section 508 of the Rehabilitation Act.

- Single Sign-On
- Personalized Content
- Content Management
- Near Real-Time Syndication
- 2-Factor Authentication (2FA)
- Access Logging
- Optimized Content Search
- Application Store
- Automated Workflows
- Real-Time Analytics
- Site Analytics

IOP Digital Toolkit - Free User experience digital toolkit
Reusable components for quick deployment of websites, portals and applications. Universal framework for developers and designers. Consistent and compliant User experiences.

- Mobile Ready
- Real-Time Analytics
- Style Guide
- Customizable Features
- Sample Code
- ADA-Compliant
- Standardized Dynamic Templates

4.2.3. Data and Analytics Products

IOP Applied Analytics
Provides the ability to build analytical and reporting solutions and deploy them in the most impactful manner possible by putting data in the hands of Users in their natural workflow. The applied analytics solution enables User to move from concept to results.

- BI Reporting
- Query Exploration
- Data Science
- Visual Analytics
- Embedded Analytics

IOP Data Integration
Provides the capability to combine information from a wide array of sources, applications and formats so that it can be analyzed to derive valuable business insights. Furthermore, data ingestion pipelines can be automated and governed, while ensuring secured access to the data.

- Data Gateways
- Workload Automation
- Data Ingestion
- Real-time Streaming

IOP Data Management
Provides rich and secure capabilities to harness the power of the analytics platform leveraging user friendly and pre-configured technologies. Additionally, the product supports a bring-your-own-tool approach allowing analysts and data scientists to work on the platform with the technologies they are most comfortable using.

- Audit
- Data Catalog
- Data Prep and Profile
- Data Warehousing
- Relational Search
- Bring Your Own Tool
- Data Lineage
- Data Sharing
- De-identification
- Code Management
- Data Portability
- Data Transformation
- Entity Resolution

IOP Service Offerings
Services, support, and training to successfully engage and onboard agencies to perform applied analytics work on the Platform.

- DataOhio Portal
- Data Onboarding
- Development Services
- Engagement
- Project Support
- Solution Design & Architecture
- Training Resources
- Use Case Development

Please explain how the InnovateOhio Platform will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.3. Enterprise Application Services

4.3.1. Application Services

Application Services provides standardized, integrated solutions for Application Development. The core components of the solution include:

- **Application Development Lifecycle Services** for creating new applications and systems.
- **Application Development Operations** for maintaining and enhancing existing applications and systems.
- **Website Lifecycle Services** for designing and creating new websites.
- **Website Operations** for maintaining and updating existing websites.
- **User Interface/User Experience Services** that work in connection with Application Development and Website work that define the "look and feel" of what users interact with.

Supporting Technology Services which support the Applications, Systems and Websites developed. These services can include payment processing, application performance monitoring, and complex reporting/visualizations.

4.3.2. Enterprise Hosted Document Management

The Enterprise Hosted Document Management is a standardized, integrated solution for document and content management. The core components of the solution include:

- **Document Management** core capabilities such as: secure check-in / check-out, version control, and index services for business documents, audio / video files, and Environmental Systems Research Institute (ESRI) / Geographic Information Systems (GIS) maps.
- **Image Processing** for capturing, transforming and managing images of paper documents via scanning and / or intelligent character recognition technologies such as Optical Character Recognition.
- **Workflow / Business Process Management (BPM)** for supporting business processes, routing content, assigning work tasks and creating audit trails.
- **Records Management** for long-term retention of content through automation and policy, ensuring legal, regulatory and industry compliance.
- **Web Content Management (WCM)** for controlling content including content creation functions, such as templating, workflow and change management and content deployment functions that deliver content to Web servers.
- **Extended Components** can include one or more of the following: Digital Asset Management (DAM), Document Composition, eForms, search, content and analytics, email, and information archiving.

4.3.3. Electronic Data Interchange (EDI) Application Integration

The EDI Application Integration service is a combination of Application Integration, Data Exchange and Electronic Data Interchange (EDI) functionality. This service provides application to application connectivity to support interoperable communication, data transformation, and business process orchestration amongst applications on the same or different computing platforms. Business process orchestration between many data formats may be supported including Web Services, XML, People-Soft, FTP, HTTP, MSMQ, SQL, Oracle, Flat File, SAP, DB2, CICS, EDI, HIPAA, HL7, Rosetta Net, etc.

The Data Exchange component allows unattended delivery of any electronic data format to a customer via encrypted files over public FTP, FTPS, SFTP, VPN.

Application Integration services are offered via:

- **End Points** – also referred to as a mailbox, this is a connectivity point to facilitate the movement or transaction of data between two or more entities.
- **KBs** – represents the size in kilobytes of a message that is transformed or processed. This typically refers to a document or file conversion or a format change.
- **Messages** – a discrete unit of data that is moved or transacted between two or more entities. A message typically represents a business document or a file.

4.3.4. Enterprise Business Intelligence

The State of Ohio Enterprise Business Intelligence (BI) service provides reporting, data visualization, enterprise data warehousing, business and predictive analytics, and decision support solutions to Users from all **120+** state agencies, boards and commissions, and institutions of higher education. With tools such as **Cognos** and **Tableau**, the Enterprise BI team can help turn raw data into usable information and powerful visualizations, in turn helping Users analyze policies and programs, evaluate operations and drive decisions.

Enterprise BI Solutions — Standardized reporting solutions to benefit all Agencies.

- **Financial Information Cost and Spend Management** – Agencies can gain valuable insights into planned, actual, and forecasted spending based on historical information as well as planned expenditures, budgets, and actual results.
- **Workforce and Human Resources** – Agencies can gain valuable insights into position management, workforce composition, pay, leave and benefits, and more.
- **Targeted Solutions** – The BI Team currently provides data visualization solutions to Agencies and custom reporting solutions to 50+ Agencies, with availability for additional options ranging from consultations through turn-key content delivery.

BI Core Reporting Services include:

Financial Information

- Enterprise Financial Dashboards
- General Ledger
- Budget and Planning (BPM)
- Travel and Expense
- Procure to Pay
- Accounts Receivable
- Asset Management
- Value Management
- Trends and Forecasts
- Statewide Cost Allocation Plan (SWCAP)
- MBE/EDGE and Equal Opportunity
- State of Ohio Payroll Projection Systems (SOPPS)

Workforce and Human Resources

- Enterprise HR Dashboards
- Workforce Profile
- Compensation
- ePerformance/ePAR
- Enterprise Learning Management

50+ Targeted Solutions including:

- Interactive Budget OBM
- Higher Education OHDE
- JFS dashboards
- State Health Facts
- BWC Core Reporting

4.3.5. eLicense Ohio Professional Licensure

eLicense Ohio Professional Licensure is the State of Ohio's online system used to manage the issuance, certifications, inspections, renewals and administration of professional licenses across the State. The eLicense application is a public/business facing system that is designed to foster the creation and growth of businesses in the State and is the mechanism through which state agencies, boards and commissions support Ohioans. The system is a central repository for license and certificate data, in addition to managing the generation and storage of correspondence. Secure fee collection is performed through an on-line payment processor, which includes bank transfers, credit cards, and other payment types.

Core system capabilities include:

Customer Relationship Manager (CRM)
- Contact Management

Revenue
- Deposit Accounting Revenue Tracking
- Refund and Reimbursement Processing
- Fine and Penalty Tracking

License Administration
- Administration
- Workflow
- Reports

Enforcement
- Enforcement Activities
- Case Management Activities

Online Licensure Services
- Applications
- Renewals
- License Verification
- License Maintenance
- License Lookup Website
- Workflow
- Document Management
- Secure Payment Processing

Other Services
- Continuing Education Tracking
- Examinations
- Inspections
- Complaint Management

4.3.6. ePayment Business Solutions

DAS OIT's ePayment Business Solution allows State agencies as well as boards and commissions to accept electronic credit card and Automated Clearing House (ACH) payments from customers. The ePayment solution is a highly flexible payment engine supporting a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, remote capture and cash payments.

The solution utilizes a single, common gateway to permit the acceptance of payments from multiple client application sources: Web, IVR, kiosk, POS, mobile, over the counter, etc. Payment processing is supported through multiple credit card gateway options, automated clearing house (ACH) bank processing, and check acceptance services.

The ePayment solution is compliant with the Payment Card Industry Data Security Standard (PCI DSS), the Electronic Fund Transfer Act (EFTA) and is audited to the standards of Statement on Standards for Attestation Engagements (SSAE) 18 SOC 1 Type II.

4.3.7. Enterprise eSignature Service

OneSpan Sign is Ohio's enterprise solution for eSignatures. The product is a FedRAMP SaaS (Software as a Service) solution, which offers a standardized approach to cloud security. OneSpan Sign's eSignature functions include workflows, tracking, audit logs and protection against forgery/non-repudiation.

OneSpan Sign has an extensive library of open application programming interfaces (APIs) to integrate eSignatures with existing applications and core systems. OneSpan Sign's pre-built, third-party connectors enable the eSignature capabilities into business software products such as Dynamics CRM, Salesforce, Microsoft SharePoint, etc.

4.3.8. Identity Management

Identity Management provides integrated authentication services across multiple enterprise service offerings. The service also streamlines the life cycle events for user credentials including onboarding, provisioning, administration, service consumption, change events, de-provisioning and off-boarding.

Identity Management is made up of four service functions:
- **Identity Repository** offers a centralized container for all user credentials and management tools for the administration of those credentials and credential attributes.
- **Core Shared Services** leverage the centralized credential from the identity repository for authentication. Service provisioning tools are available to provision access to various portions of the core shared services within the Identity Management service.

- **Application Integration** permits an Agency's line of business application to authenticate to the centralized user credential within the Identity Repository using a secure Lightweight Directory Access Protocol (LDAP) and/or Active Directory Federation (SAML 2.0)
- **Endpoint Consumption** allows for the placement of desktops, laptops, and/or tablets to reside within the Identity Management service. This extends the ability to use a single credential to authenticate to workstations and applications.

4.3.9. IT Service Management Tool (ServiceNow)

DAS OIT offers **ServiceNow**, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk work-flow based application which provides flexibility and ease-of-use. The IT Service Management Tool provides workflows aligning with Information Technology Infrastructure Library (ITIL) processes such as incident management, request fulfillment, problem management, change management and service catalog. These processes allow customers to manage related fields, approvals, escalations, notifications, and reporting needs. Customers have the option of provisioning the entire suite of service features or selecting those features best suited for their needs.

The following modules are currently in use on the enterprise platform:

- IT Service Management
- IT Operations Management
- IT Business Management
- Governance, Risk & Compliance
- Security Operations
- Intelligent Applications

ServiceNow Product Catalog

The Product Catalog contains:

- The applications currently in use of the State of Ohio ServiceNow Application across Agencies
- The product wheel of the platform footprint
- Applications in use by Agencies
- Product descriptions by Platform family, then Application within Family for current functionality
- Product descriptions by Platform family, then Application within the Family for services not deployed

4.3.10. Automated Ticketing

DAS OIT offers Watson Automated Ticketing that integrates with ServiceNow for Agencies interested in having incidents and requests in their UNASSIGNED queue that comes through email assigned to the proper resolver queue. This service will route these incidents to the appropriated queue based on historical data and optionally provide other use cases as well. Watson is a cognitive automation platform that leverages machine learning, natural language processing, deep learning, semantic ontologies, pattern recognition, etc.

Watson is used for automating manual parts of the support processes using Artificial Intelligence algorithms. It automates processes to provide more efficient operation with higher quality results compared to manual performance.

4.3.11. Ohio Benefits

Ohio Benefits provides a comprehensive and effective platform for planning, designing, development, deployment, hosting and ongoing maintenance of all State of Ohio Health and Human Services (HHS) Public Assistance Services and Programs.

Ohio Benefits provides superior eligibility services including citizen self-service, efficient workflow management and coordination, an agile and easily manageable rules engine, improved data quality and decision support capabilities. Ohio Benefits supports improvement in state and county productivity, capability and accessibility of benefits to Ohioans through a robust enterprise system.

The Ohio Benefits platform provides four distinct technology domains:

- **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- **Enterprise Information Exchange** – Discovery Services (Application and Data Integration, Master Data Management (MDM) Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management
- **Analytics and Business Intelligence** – Integration and delivery of analytics through alerts, notifications & reports.
- **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs.

Privacy and security are the foundational blocks of the platform which is compliant with all State and federal standards.

4.3.12. Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time and money saving online filing and payment system that simplifies business' relationships with government Agencies.

Ohio businesses can use OBG to access various services and electronically submit transactions and payments with many Agencies. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

OBG Electronic Filing routes data and payment information directly to program administrators at the Agencies so that they may continue to manage the overall account relationship.

Businesses must be registered with an Agency before using OBG Electronic Filing. Selected Agency registrations are available through OBG Electronic Filing. Information about other registrations may be obtained by visiting the 'Starting a Business' section of the Ohio Business Gateway (http://business.ohio.gov/). If a registration is not offered on OBG Electronic Filing, the administering Agency will provide information on how to obtain the registration necessary to begin using OBG Electronic Filing services. For Municipal Income Tax Electronic Filing, businesses must first register directly with municipalities before using OBG.

4.3.13. Ohio Administrative Knowledge System (OAKS)

The Ohio Administrative Knowledge System (OAKS) is the State's Enterprise Resource Planning (ERP) system which provides central administrative business services such as Financial Management, Human Capital Management, Content Management, Talent Management, Enterprise Learning Management and Customer Relationship Management.

Core system capabilities include:

Content Management (myohio.gov)

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids and news
- Statewide News
- Password Reset for Active Directory

Customer Relationship Management (CRM)

- Contact / Call Center Management

Enterprise Business Intelligence

- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven reporting

Ohio Recruit

- 24x7 Recruiting, Reporting and Analytics
- Applicant Tracking and Compliance

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eSourcing
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement

- Targeted Business Intelligence
- Tableau Analytics and Visualization

Ohio Learn
- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting
- **NEW**: Ability to extend Training Content to External Learners

- Travel & Expense

Human Capital Management (HCM)
- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration

4.3.14. Enterprise Geocoding

OAKS Enterprise Geocoding is the process of determining associated geographic coordinates from other geographic data, such as street addresses or zip codes. With these geographic coordinates, the features can be displayed and analyzed in a Geographic Information Systems (GIS), or the coordinates can be embedded into media such as digital photographs via geotagging.

OAKS Enterprise Geocoding combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for on-line applications or large numbers of addresses can be processed in batch mode. The quality of each address is improved by standardizing it to meet stringent U.S. Postal Service standards.

Leveraging address location information developed and maintained by local government, the OAKS Enterprise Geocoding uses a multi-tiered geocoding process incorporating data from multiple entities to provide Agencies with the most accurate location information available.

4.3.15. Geographic Information Systems (GIS) Hosting

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Customers can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications. GIS enhances decision support, integrating data from a variety of sources to be analyzed spatially with the results presented in the form of a map.

DAS OIT offers three types of hosted GIS services:

- **Geodata Hosting** provides a platform for customers to deliver online spatial data and content to end users or applications. Online spatial data can be consumed by desktop GIS applications and web-based applications.
- **Geoprocessing** provides access to server-side geoprocessing tools that allow users to publish analytical models for use within desktop applications by remote users or embedded within Internet mapping applications.
- **GIS Map Application** Hosting provides a platform for customers to deliver web-based mapping content to end users.

GIS Hosting can be combined with the Enterprise Geocoding to create a comprehensive web application to locate and display events, customers, or Agency assets on a map in a browser.

Please explain how the State's Enterprise Application Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.4. Hosted Services

4.4.1. Enterprise SharePoint

The Enterprise SharePoint Service supports both an on premises and cloud environment. Enterprise SharePoint service provides Site Administration, Technical Services/Support for SharePoint and third-party tools (e.g., Nintex) as well as Strategy, Adoption, Operations and Strategic Management within both the Tenant and Farm level for SharePoint related services. Key Services Included: Site Administration and Technical Services:

Basic Services include:

- Site Collection Creation
- How to's from Site Collection Admin/users
- Research Apps and make available to Tenant/Farm
- Consult on SharePoint Online and On Premises needs with Agencies
- Review & Approve 3rd party tool integration
- Incident/Problem Resolution
- Work to eradicate issues in SharePoint Online
- Routine maintenance
- Site to Site Migrations

Additional Services Available:

- Customized Search
- Site Branding & Design
- Migrating content from one environment to SharePoint (e.g., FileShare to OneDrive or SharePoint)
- Rights Management & Data Protection
- Retention Management
- Azure integration
- Customized Applications and Workflows
- Content types, managed metadata, site structure and navigation

Strategy, Operations and Management – Key Services include:

- Program Management
- SOW and contract creation and processing
- Contract Management
- Adoption Service Template & Education
- Lunch 'n Learns
- Yearly Reporting
- Community Center Intranet Site Management

Services performed for On Premises environment only:

- Configuration Management
- Code Management
- Patching and Software updates
- Farm Backup and Restore
- Refreshing Content Across Development and Staging environments
- Physical Architecture Changes

4.4.2. Database Support

Database Support provides technical assistance for database implementation and usage. Services utilized by customers may include any or all of the following service offerings: installation, upgrade and management of database software, database administration tools and packaged application database products, backup/recovery procedure implementation, monitoring, tuning and troubleshooting.

Please explain how the State's Hosted Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.5. IT Security Services

4.5.1. Secure Sockets Layer Digital Certificate Provisioning

Secure Sockets Layer (SSL) Digital Certificate Provisioning service provides Secure Sockets Layer Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes for each designated customer Agency while leveraging a common portal.

In addition, please review the Security Supplement (Supplement S - State Information Security and Privacy Requirements and State Data Handling Requirements).

Please explain how the State's IT Security Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.6. Messaging Services

4.6.1. Microsoft License Administration (Office 365)

The Office 365 service provides customers the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing the customer to access services virtually anytime and from anywhere and includes email archiving and eDiscovery services.

The Office 365 service provides licensing and support for email, Office 365 ProPlus (Outlook, Word, Excel, PowerPoint, Publisher, Teams and OneNote), SharePoint, and OneDrive for Business. Please note that the Office Suite may require agency deployment or agency/end user installation as well as patch management and distribution.

- Email in the Microsoft Cloud
- Office 365 ProPlus
- Teams
- SharePoint Online
- OneDrive for Business

Please explain how the State's Messaging Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.7. Network Services

Offeror's solutions must work within the State's LAN / WAN infrastructure.

4.7.1. Ohio One Network

The State of Ohio's One Network is a unified solution that brings together design, engineering, operations, service delivery, security, mobility, management, and network infrastructure to target and solve key government challenges by focusing on processes, procedures, consistency, and accountability across all aspects of state, city and local government.

Ohio One Network can deliver an enterprise network access experience for their customers regardless of location or device and deliver a consistent, reliable network access method.

4.7.2. Secure Authentication

The DAS OIT Secure Authentication service provides a managed two-factor user authentication solution to protect an Agency's resource. The authentication function requires the user to identify themselves with two unique factors, something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to a customer's environment.

4.7.3. Wireless as a Service

Wireless as a Service is the IT Enterprise Wireless hosted network which allows customers to connect laptops and devices to their data via a wireless interface. This service is an all-inclusive enterprise level wireless LAN solution that offers guest, employee, voice and location-based services with 24/7 target availability.

Coverage is three tiered:

- Broad coverage – small number of Users with low throughput, i.e., public hot spot, warehouse.
- General data use – most common, general computing with robust data performance.
- High-capacity use (Voice) – maximum capacity, high bandwidth Users, i.e., location and tracking service.

Please explain how the State's Network Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

4.8. Telephony Services

4.8.1. Voice Services – VoIP

The State of Ohio hosted cloud VoIP service, also known as NGTS (Next Generation Telephony Service) provides core telephony, voice mail, e911, collaboration, video, audio, conferencing, and auto attendant functions. Optional services include automatic call distributor (ACD), interactive voice response (IVR), multi-channel contact center solutions and session initiation protocol (SIP) trunking among a variety of other features. The service was the first business class phone system to offer closed captioning for the hearing impaired, and also includes features for those with vision and mobility impairments.

The following voice services are offered in addition to the State's hosted VoIP service.

4.8.2. Toll-Free Service

This service provides the capability to incur telephone charges for incoming calls to an 8xx number.

4.8.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers

The Contact Center Enterprise allows callers to fill in CRM forms with information prior to an Agent responding. With IVR and Advanced Data Collection, callers will spend less time in Call Queues. However, during high demand times, callers can be put on Virtual Hold allowing callers to receive a call back when Agents become available. Call

recording with screen capture allows the User to monitor, record, store, and QA calls, helping insure a consistent service experience.

This service also includes multi-channel communications including chat, text, SMS and email to afford those trying to contact the State the ability to contact the State in a variety of ways.

4.8.4. Call Recording

This service is available for new VoIP profiles or modifying existing profiles.

4.8.5. Conferencing

This service offers a conferencing service via telephone lines and or TCP/IP networks. It provides voice & video conferencing capabilities within the network and participants can also join in from outside the network.

4.8.6. Fax2Mail

The Fax2Mail is a “hosted” fax solution that allows organizations to seamlessly integrate inbound and outbound fax with their existing desktop email and back-office environments. The Fax2Mail is completely “cloud-based” (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. The Fax2Mail solves all faxing requirements, including inbound and out-bound fax, both at the computer desktop and from/to back-office systems, ERP applications, and electronic workflows.

4.8.7. Session Initiation Protocol (SIP) Call Paths

The Session Initiation Protocol Call Paths is used to allocate bandwidth. SIP Call paths:

- Provide existing telephony infrastructure with NGTS services.
- Extends infrastructure into the NGTS cloud.
- Leverages existing investment.
- Bridges the gap.
- All of the United States are Local Calls.
- Share video and collaboration.
- Leverage Toll Free offering.
- Centralized trunk savings.

4.8.8. Site Survivability

This service provides reliable communications via multi-feature redundancy for centralized call processing.

4.8.9. VoIP related Professional Services and Training

Training services can be requested for VoIP telephone Users.
Professional services are also available for planning and migration of large contact centers, and for integration of contact centers with cloud services including Salesforce.

Please explain how the State’s Telephony Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be identified in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements

If an offeror needs to request a variance from a State IT Policy, Standard or Service requirement outlined in this supplement, please provide a rationale and an overview for each request in the table below.

Section Reference	IT Policy, Standard or Service Requirement	Rationale for Proposed Variance from Requirement	Proposed Variance Overview
Example: **Section 4.3 Enterprise Application Services - Enterprise eSignature Service**	**Example**: The offeror shall use the State's eSignature solution.	**Example:** An eSignature solution is already integrated into the proposed solution. Using the State's service would result in increased cost due to integration complexities, as well as additional testing and resource needs. It would also result in longer deliverable timeframe.	**Example:** The Offeror's eSignature solution provides the same capabilities as the State's required solution. The Offeror's solution includes a workflow component and an eSignature User interface.

DATA SECURITY AND PRIVACY TERMS

These Data Security and Privacy Terms ("Terms") describe the responsibilities for the Contractor relating to State information security and privacy standards and requirements for all proposed solutions, whether cloud, on-premises, or hybrid based. These Terms applies to all work and services across all environments, and State of Ohio ("State") and Contractor locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in performing the work, and any Contractor access to State resources in conjunction with the delivery of work.

The Contractor must comply with the State IT Security Policies and Standards and these Terms and must accept the security and privacy requirements outlined in these Terms in their entirety, as they apply to the services being provided to the State. The Contractor will be responsible for maintaining information security in any environments under the Contractor's management in accordance with State IT Security Policies and Standards.

These Terms apply to the following:

A. Major and minor projects, upgrades, updates, fixes, patches, and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State.
B. Any systems development, integration, operations, and maintenance activities performed by the Contractor.
C. Any authorized change orders, statements of work, renewals, or amendments to the Contract.
D. Contractor locations, equipment, and personnel that access State systems, networks, or State Data directly or indirectly.
E. Any Contractor personnel that have access to State Data.

These Terms are in addition to the Contract terms and conditions. In the event of a conflict between the Contract and these Terms, the most stringent standard will prevail.

Definitions

1. **Contractor** for purposes of these Terms, includes subcontractors or other personnel under the authority or control of the Contractor performing the work or providing the services under this Contract.

2. **Personally Identifiable Information** means information that can be used directly or in combination with other information to identify a particular individual. It includes:
   A. A name, identifying number, symbol, or other identifier assigned to a person,
   B. Any information that describes anything about a person,
   C. Any information that indicates actions done by or to a person,
   D. Any information that indicates that a person possesses certain personal characteristics,
   E. The definitions of "personal information" in Revised Code chapters 1347.01, 1347.04 through 1347.99, and
   F. The various other definitions of "personal information" throughout the Ohio Revised Code.

3. **Security Event** has the meaning set forth in Section 7 of these Terms.

4. **Security Incident** has the meaning set forth in Section 7 of these Terms.

5. **State Data** means all data and information provided by, created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.

6. **Sensitive Data** means any type of data that presents a high or moderate degree of risk if released, disclosed, modified, or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a

moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure.

Sensitive Data includes, but is not limited to:

A. Personally Identifiable Information (PII);
B. Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);
C. Federal Tax Information (FTI) under IRS Publication 1075 - Tax Information Security Guidelines for federal, state, and local agencies;
D. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); United States Code 42 U.S.C. 1320d through 1320d-9 (HIPAA); and Code of Federal Regulations for Public Health and Public Welfare: 42 C.F.R. 431.300, 431.302, 431.305, 431.306, 435.945, 45 C.F.R. 164.502(e) and 164.504(e);
E. Criminal Justice Information (CJI) under the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy available at https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center;
F. Payment Card Industry Data Security Standards;
G. Social Security Administration (SSA) Data which is data received by the State from the Social Security Administration in accordance with the current Computer Matching and Privacy Protection Act between the State of Ohio and the Social Security Administration; and
H. Other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

7. **State IT Security Policies and Standards** means the policies and standards available at https://das.ohio.gov/technology-and-strategy/information-security-privacy/information-security-governance.

Requirements

1. The Contractor's Responsibilities Generally

The Contractor is responsible for maintaining the security of information in accordance with the applicable security baseline of the current published version of the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," ("NIST 800-53") commensurate with the type of State Data involved in the Contract as communicated by the State. If the State is providing the network layer, the Contractor must be responsible for maintaining the security of the information in environment elements that are accessed, utilized, developed, or managed by the Contractor. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in the Contract, adhere to State IT Security Policies and Standards, and use procedures in a manner that does not diminish established State capabilities and standards. All work performed by the Contractor, all deliverables provided by the Contractor, and all environments utilized to perform the Contractor's work must comply with State IT Security Policies and Standards. The Contractor's information security and technology responsibilities with respect to the work and services the Contractor is providing to the State include the following, where applicable:

A. Support State IT security policies, standards and procedures development and maintenance activities. Assist in the implementation of associated security procedures with the State's review and approval, including physical access requirements, User ID approval procedures, and a Security Incident action and response plan.

B. Support implementation and compliance monitoring as per State IT Security Policies and Standards.

C. Upon identification of a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify

and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

2. Protection and Handling of State Data

Contractor shall maintain an Information Security Program ("ISP") made up of policies, procedures, technical and organizational safeguards, and training designed to protect State Data against unauthorized loss, destruction, alteration, access, or disclosure. To protect State Data, the Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect State Data from unauthorized disclosure, modification, use or destruction. To accomplish this, the Contractor must adhere to the following requirements regarding State Data in addition to the confidentiality requirements in the Contract:

A. Assume all State Data is both confidential and critical for State operations.

B. Maintain, in confidence, State Data it may obtain, maintain, process, or otherwise receive from or through the State during, and pursuant to, the provisions of the Contract and these Terms.

C. Use and permit its employees, officers, agents, and subcontractors to use any State Data received from the State solely to perform its obligations under the Contract.

D. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and sub-contractors to sell, rent, lease, or disclose, any such State Data to any third party, except as permitted under the Contract or required by applicable law, regulation, or court order.

E. Take all commercially reasonable steps to (a) protect the confidentiality of State Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to State Data received by the Contractor from the State.

F. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of State Data.

G. Ensure that internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data, and periodically review and update these policies, plans, and procedures as needed.

All State Data at rest in systems supporting the Contractor's services must reside within the contiguous United States with a minimum of two data center facilities at two different and distant geographic locations and be handled in accordance with the requirements of these Terms at all Contractor locations.

If the Contractor will be handling Sensitive Data, the State may require additional documentation such as the Contractor's information security policies and procedures, contingency plans, or incident response plans, a Privacy Impact Assessment (PIA), FIPS-199 compliance documentation, a NIST-compliant System Security Plan (SSP), and Plans of Action and Milestones (POA&M) documentation.

3. Security Standards and Warranties

All solutions shall operate at the *moderate level baseline* as defined in the current published version of NIST 800-53, be consistent with Federal Information Security Management Act, 44 U.S.C. § 3551 et seq. ("FISMA 2014") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications.

Contractor's information security program protects State Data by aligning with NIST 800-53 to implement an industry security and privacy standard including, at a minimum:

A. Security and confidentiality of State Data.

B. Protection against anticipated threats or hazards to the security or integrity of State Data.

C. Protection against the unauthorized access to, disclosure of, or use of State Data.

D. Give access to State Data only to those individual employees, officers, agents, and sub-contractors who need to know such information in connection with the performance of the obligations under the Contract.

E. Cooperate with any attempt by the State to monitor compliance with the foregoing obligations as reasonably requested by the State.

F. Promptly destroy or return to the State, in a format designated by the State, all State Data received from or through the State upon completion of the work under the Contract or upon termination or expiration of the Contract.

G. Maintain appropriate and effective business continuity and disaster recovery plans to ensure resiliency of State Data and business operations.

H. Maintain a privacy policy that includes, at a minimum, processes for the State to obtain individual privacy consent for the use of PII, at the determination of the State, and to respond to individuals' requests to access, correct, and delete their PII unless otherwise expressly agreed to in the Contract. All PII, including PII that has been de-identified, is considered State Data and Confidential Information under this Contract.

Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made, and must promptly remediate any and all vulnerabilities and provide the State with patches to address the vulnerabilities at no cost to the State. Contractor must follow best practices for application code review and the most current version of the Open Source Foundation for Application Security (OWASP) top 10.

In addition to the warranties provided and pursuant to the terms of the warranties section of the Contract (i.e., notification, correction, and indemnification), Contractor warrants that its software and/or service are free from any and all defects in materials, workmanship, and design. Contractor warrants that the software is free from any and all viruses, malware, and other harmful or malicious code.

4. Permitted Disclosure to Third Parties

Disclosure of State Data is permitted as set forth in the Contract. Additionally, disclosure of State Data is also permitted when required by applicable law, regulation, court order or subpoena. If the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Sensitive Data or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, the Contractor must notify the State within 24 hours of receipt of the order or request in order for the State to seek a protective order or take other appropriate action, as desired. The Contractor must also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State.

If, in the absence of a protective order, the Contractor is compelled as a matter of law to disclose the information provided by the State, the Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, the Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and

the nature of wording of such disclosure) and must use commercially reasonable efforts to obtain confidential treatment for the information disclosed.

The Contractor may disclose Confidential Information to the following people, subject to the requirements of the Contract and these Terms:

A. To State or Federal auditors or regulators.

B. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

C. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

5. Auditing

A. The Contractor must obtain an annual audit of the services being provided under this Contract that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The audit must cover all operations pertaining to the services covered by this Contract. The audit will be at the sole expense of the Contractor and the results must be provided to the State within 30 days of Contractor's receipt of its audit results each year.

B. The State may, at any time in its sole discretion, elect to perform a Security and Data Protection Audit. This includes a thorough review of Contractor controls, security and privacy functions and procedures, data storage and encryption methods, and backup and restoration processes. The State may utilize a third-party contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met. The State will provide its request in writing and will work with the Contractor to schedule time to conduct the audit.

C. At no cost to the State, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the services provided under this Contract.

6. Background Investigations of Contractor Personnel

The State of Ohio may conduct background investigations on Contractor personnel that may have access to State Data or as otherwise deemed necessary by the State. Any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (c) has been convicted of a felony may not perform certain services under the Contract. Contractor personnel who will have access to FTI or CJI must complete required background investigations that are favorably determined prior to being permitted to access the information. In addition, existing Contractors whose personnel already have access to FTI or CJI that have not completed the required background investigations within the last five years must complete the required background investigations that are favorably adjudicated prior to being permitted continued access to the information. If any Contractor personnel with existing access to the information have an unfavorably adjudicated background investigation completed, the State may terminate that personnel's access to the information.

7. Security Incidents

A. Definitions. A security incident threatens the confidentiality, integrity, or availability of State information resources. A "Security Incident" means there is a successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. A "Security Event" is any observable occurrence that is relevant to information

security within normal operational noise levels and below pre-defined incident thresholds.

Security Incidents may fall into one or more of, but are not limited to, the following categories:

i. Loss or Theft
ii. Denial of Service (DoS)
iii. Improper Usage or Access
iv. Information Spillage
v. Malicious Code
vi. Phishing Messages
vii. Scans/Probes/Attempted Access
viii. Social Engineering
ix. Unauthorized Access

Security Events may fall into one or more of, but are not limited to, the following:

i. unsuccessful log-on attempts,
ii. unsuccessful denial of service attacks,
iii. unsuccessful phishing attacks, and
iv. unsuccessful network attacks such as pings, probes of firewalls, and port scans.

B. Security Incident Response and Reporting

The Contractor is responsible for Security Incident response, including containment, eradication, and recovery, to minimize the impact to the State. In addition to the requirements in the Contract, the Contractor must perform the following in response to a Security Incident involving State Data.

The Contractor is not required to report Security Events which do not adversely impact or potentially impact State Data or information systems unless a pattern of attacks significantly increases the risk of impact. Contractor must report in writing to the State within 24 hours of the Contractor becoming aware of any Security Incident and/or use or disclosure of State Data not authorized by the Contract, including any reasonable belief that unauthorized access to or acquisition of the State Data has occurred, and fully cooperate with the State to mitigate the consequences of the Security Incident. Within five business days of the initial Security Incident report to the State, the Contractor must document and begin providing follow-up reports for all Security Incidents to the State. The Contractor must provide updates to the follow-up reports until the investigation is complete. At a minimum, the Security Incident reports will include:

i. Data elements involved, the extent of the State Data involved in the Security Incident, and the identification of affected individuals, if applicable.

ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed State Data, or to have been responsible for the Security Incident.

iii. A description of where the State Data is believed to have been improperly transmitted, sent, or utilized, if applicable.

iv. A description of the probable causes of the Security Incident and, in the final report, the root cause.

v. A description of the proposed plan for preventing similar future Security Incidents, including a recommended risk remediation plan.

vi. A description of the corrective actions taken, including repair (elimination of a defect or incident and/or restoration of system functionality requirements according to the Contract) and resolution (a temporary workaround to enable system function).

vii. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.

The Contractor must comply with all applicable laws that require the notification of individuals, or with other reasonable direction of the State for notification, in the event of a Security Incident involving personally identifiable information, or any other event requiring such notification. The State may, in its sole discretion, choose to provide notice to any or all parties affected by a Security Incident, but the Contractor shall reimburse the State for the cost of providing such notification. Contractor further agrees to provide, or to reimburse the State for its costs in providing, any credit monitoring or similar services that are necessary as a result of Contractor's Security Incident. Under Ohio law, State Data is State property and any illegal activity involving State property is subject to a criminal investigation. The Contractor shall preserve sufficient evidence to ensure accurate Security Incident records, facilitate an investigation, and determine the extent of the Security Incident.

The Contractor shall work with the customer State agency to establish a Security Incident reporting communications procedure including Contractor and customer State agency contacts, communication methods and tools. If there is no procedure established, the Contractor must report Security Incidents to the primary contact listed in the Contract or that contact's successor and Contractor must report the Security Incident to the State via email at Enterprise.SIRT@das.ohio.gov or call 614.728.7448.

The State reserves the right to conduct an independent investigation of the Security Incident, and the Contractor shall cooperate with the investigation. The independent investigation may be conducted by a State agency or a third party acting on behalf of the State.