Innovative Solutions for the Office of Unemployment Insurance Operations (OUIO)
Request for Quote
JFS-RFQ-2021-14-8185
August 12, 2020

This Request for Quote (RFQ) is posted to seek vendors, preferably Ohio companies, to manage multiple COVID-19 emergency response initiatives for the Ohio Department of Job and Family Services (ODJFS) Office of Unemployment Insurance Operations (OUIO). As a result of COVID-19, OUIO experienced unprecedented volumes that have impacted claimant's ability to receive unemployment benefits in a timely manner. This is mainly due to challenges with adjudication and the lack of fully trained resources required to facilitate inquiries. As a result, we are seeking additional technology solutions to assist with the processing and resolution of claims. The selected vendor for the project will work with ODJFS to accomplish four objectives:

1. Self-service adjudication capabilities;
2. A virtual assistant (web and mobile) to provide guidance through self-adjudication;
3. A virtual assistant in the contact center to address easier self-service items; and
4. Implementation of preventative measures to prevent potential issues that would require adjudication.

Request for Quote JFS-RFQ-is issued by the ODJFS, Office of Contracts and Acquisitions (OCA) in response to the COVID-19 to establish an emergency contract. This is an open market opportunity with a preference for Ohio companies. For this solicitation only, interested vendors are encouraged to propose the use of current agreements with the State of Ohio to govern the quote being provided. In addition, vendors are invited to respond with a company letterhead quote for "Innovative Solutions for the Office of Unemployment Insurance Operations".

Please carefully review details within this document prior to submitting your company quote. The vendor quote must include the following for evaluation and award considerations:

1. Quote must be valid for 90 days and provided on Company Letterhead and must contain contact name, business phone number(s) and e-mail address.
2. Quote must include a statement that the prices are firm, fixed fees.
3. Vendor must not submit a proprietary or confidential quote.
4. Vendors must agree to leverage the attached ODJFS contract template with no exceptions unless leveraging a current agreement with the State of Ohio or public sector. Vendors may sign and date the attached ODJFS contract to expedite the signature process, if selected.
5. Vendors who propose to use a current agreement with the State of Ohio or public sector must include the fully executed agreement with the quote.
6. Vendors must include any proposed software licensing as an attachment to its Quote.
7. Vendors must complete and sign the Offshore waiver attached to the RFQ.
8. Vendors must concisely describe its organization experience and capabilities including any subcontractors proposed to deliver the solutions as described in the RFQ. Please limit the description to no more than 2 pages
9. Vendors must include their response a concise description of the proposed staff experience and capabilities requirements (including any subcontractors) and include resumes of key staff.
10. Vendors must provide three customer references that include a description of the services and solutions successfully provided on projects to demonstrate meeting the mandatory qualification of having experience successfully implementing machine learning and/or artificial intelligence automation work within a contact

center environment, with demonstrated quantitative improvements and outcomes. The customer references must be current and include a phone number and email address, to allow ODJFS the opportunity to the Vendor's experience.

11. Quotes failing the mandatory qualification will be disqualified.
12. Vendor must provide, at a minimum, a statement affirming and agreeing to the required scope of services and provide descriptions of the solutions and services that will be performed to meet the objectives and requirements stated within this RFQ. Vendors are to limit the marketing material provided in its response so that the focus is on the proposed solutions and services being offered. Vendor must provide a high-level Implementation Plan, Work Breakdown Structure (WBS) and project schedule for the required solutions and services to be delivered.
13. Vendors must clearly articulate in a separate section of its response any assumptions made in preparing the response.
14. ODJFS may request interviews or presentations to validate the quote; ODJFS may request interviews/presentations from the highest-ranked vendors and reserves the right to bypass interviews and presentations altogether.
15. ODJFS will rank the vendors based on the best value including, but not limited to, the proposed solutions and services; proposed staff experience and expertise; company's experience and capacity; Proposed Implementation Plan, WBS and Project Schedule; time to market for the solutions; Ohio preference and Total Cost of Ownership inclusive of proposed fees.
16. Quote must be complete, meet the mandatory qualification and the proposed fees must be in the required format.
17. ODJFS will apply an Ohio Presence Preference to qualifying Quotes that include sufficient evidence of satisfying the Ohio Presence criteria. This preference will be applied to the proposed fees and may be used to select the winning vendor in the event that best value among multiple vendors are determined to be comparably equivalent best value by ODJFS.
18. ODJFS may not award to a vendor deemed not responsive or responsible, including not in good standing with previous clients or the public sector, has unsatisfactory references, etc.
19. RFQ Award will be based on best value and formalized via a contract between the selected vendor and ODJFS.
20. ODJFS may, at its sole discretion, waive minor errors or omissions in the quotes.
21. ODJFS reserves the right to request clarifications from vendors.
22. ODJFS may select a single vendor for contract award as a result of this RFQ or cancel the RFQ.

To respond to this request for quote, attach your company letterhead quote in an e-mail to JFS-IT-BID-REQUEST@jfs.ohio.gov with e-mail subject JFS-RFQ-2021148185 on or before 8:00 AM, Monday, August 24, 2020. **All quotes must be good for 90 days** and late e-mail responses will not be evaluated for the RFQ award. The inquiry process for this solicitation will be from Wednesday, August 12, 2020 through 8:00 AM EST Monday, August 17, 2020.

Scope of Work/Services

As a result of the COVID-19 pandemic and the unprecedented numbers of unemployed Ohioans seeking services, benefits and guidance from the Ohio Department of Job and Family Services (ODJFS) Office of Unemployment Insurance Operations (OUIO), ODJFS has entered into multiple contracts for products and services. These contracts include at a minimum:

- Services to assess, enhance and optimize the Ohio Job Insurance application to meet the surge in demand
- Implementing a solution for pandemic unemployment assistance
- Call center services to support OUIO and all impacted populations

The Vendor selected from this solicitation must not disrupt ongoing progress of inflight initiatives. The required solutions and services may be needed for up to three (3) years from the work start date.

The selected vendor will work with ODJFS to accomplish the below mentioned deliverables, with emphasis for each of these requirements to identify and implement automated processes where possible to improve contact center and adjudication efficiency. Vendors must propose deliverables in its response, following leading practices and a structured methodology for project management and implementing technology solutions. Consideration must also be given to training/knowledge transfer in the proposed approach. This section is not intended to suggest that certain requirements are more important than others.

The proposed deliverables must at a minimum include the following and must be described in the Vendor's response.

1. Project Plan;
2. Assess the current OUIO technology landscape and adjudication process and submit a comprehensive recommendation of refinements to the proposed solution and implementation plan;
3. Testing; and
4. Go-live.

Project Solutions

The RFQ requires several technology solutions to be delivered to address the Department's challenges with managing the unprecedented volume of calls. For the solutions described below, Cloud solutions are preferred, however on-premise solutions will also be considered. In addition, current technology, solution scalability, alignment with business objectives, and the Go-Live date will be significant factors in selecting the solutions.

Although the number of incoming calls is decreasing, the handle rate percentage does not appear to be increasing. Based on the data, it appears claimants are reaching agents, but they aren't being adequately helped, thus they become a repeat caller. Though ongoing internal training and staffing efforts continue for the contact center and adjudication, decreasing the need for claimants to call the contact center and/or speak with an agent regarding their claim is imperative. The purpose of these capabilities would be to aid the ODJFS self-service capacity.

- We are looking for a self-service adjudication solution. This will allow claimants to address pending adjudication issues on the web or on their mobile device in a self-service model. The concept would be to notify claimants and provide clear details of their exact adjudication issue(s), steps on how to resolve the issue(s) on their own, and the capability to fix their claim via a virtual assistant. Once the claim is fixed, logic would be added to either auto-adjudicate or send the corrected claims to a quality assurance queue for confirmation. Single messaging service or targeted messaging capabilities would be leveraged. This capability will automate the process of notifying claimants of their adjudication issue(s) (to mobile, desktop, or similar personal device), alongside providing self-service next steps. There are currently roughly 600k outstanding adjudication issues. Self-adjudication will not apply to all issue types but will reduce the need for manual adjudication and increase the speed of resolution where applicable.
- In addition to the self-service adjudication solutions described above, we are looking for the implementation of preventative methods that are easily understood and can warn claimants of potential issues before they submit their initial claim application and continued weekly check-in within the Ohio Job Insurance application. Thus, requesting that they fix the potential issue prior to submission. Confirmation alerting capabilities would be necessary to primarily ensure that claimants who are submitting forms online have effectively reviewed their claim to prevent the need for resubmission or claims denial due to an error. There are currently roughly three hundred eighty-four thousand (384,000) active unemployment claims. This count has been as high as seven hundred and twelve thousand (712,000) over the last four (4) months.
- We are also seeking a virtual assistant (web and mobile) for the contact center to address less complex self-service items (e.g., claimant weekly check-ins and inquiries on claim status) that are currently being handled by an agent or a limited IVR feature. The overall goal would be to limit calls to agents and implement a virtual assistant, with customizable self-service capabilities. Weekly check-ins include the claimant providing the necessary information to validate they are available and able to work, however still unemployed for the respective reporting week. As many as one hundred thousand (100,000) weekly claim check-ins are handled by the contact center agents monthly. The contact center also receives claim status inquiries. There is currently an Interactive Voice Response (IVR) in place to provide limited claim information to claimants. As many as five hundred and fifty thousand (550,000) claim status inquiries are handled by the contact center IVR monthly. Many of these callers proceed to speak with an agent following the IVR information provided. Expanding the claim information provided to the claimants can assist with reducing the need to speak with an agent. Providing this functionality allows the agents to focus on more critical tasks that require their subject matter expertise.
- Omnichannel capabilities, especially including chat bots, chat functionality, SMS, etc., are needed for the solutions provided.
- Robust reporting capabilities providing user experience insights (e.g., outcomes, resolution rates, call disposition, etc.) must be provided for the proposed solutions.

The technology for these solutions must be compatible with the current Ohio Job Insurance (OJI) application which is in Java and DB2 Database on Mainframe. The new Ohio Job Insurance application will be in .NET, therefore the solutions proposed should also be compatible with this technology. Please review the logical architecture diagram for the current OJI application for additional technology information.

There are currently two Contact Center environments in use by JFS. One Contact Center utilizes Cisco UCCE 10.5 and the other utilizes Amazon Web Services (AWS) Connect. The technology proposed must be compatible with both of these Contact Center environments. Please review the logical architecture diagram for additional technology information.

Microsoft BOT Framework is a preferred platform for Chatbot implementation, however other platforms will be considered.

To review the current technical environment pertaining to this solicitation Vendors must properly submit a request to ODJFS for the technical information. To obtain the information Vendors must sign the attached Non-Disclosure Agreement (Attachment A) and include it with a request for the technical information pertaining to the Innovative Solutions for the Office of Unemployment Insurance Operations (OUIO) Request for Quote JFS-RFQ-2021-14-8185. Vendors must also include the name of the requestor, company name, phone number and email address and submit the request to JFS-IT-BID-REQUEST@jfs.ohio.gov with an e-mail subject JFS-RFQ-2021148185. The deadline for requesting technical information is the same as the inquiry end time and date, 8:00 AM Monday, August 17, 2020.

Maintenance and Operations

Vendor must describe its maintenance, support and operations for the proposed solutions. This response should at a minimum adequately address hours of coverage for maintenance and technical and user support; issue management by defined severity levels and response times; and proposed SLAs, if applicable.

Ohio Presence

For purposes of this RFQ, ODJFS is applying an Ohio preference to Quotes that satisfy one of the two criteria below.

1. A vendor is an Ohio company if the company is headquartered in Ohio where services are produced/performed. Vendors are to indicate the physical address of its Ohio headquarters and the total number of Ohio and Nationwide employees, respectively.
2. A vendor has significant economic presence within the state of Ohio when the following criteria are met:
   a) Vendor has paid the required taxes due the state of Ohio.
   b) Vendor is registered with the Ohio Secretary of State. Questions regarding registration should be directed to (614) 466-3910 or visit their web site at: http://sos.state.oh.us/
   c) Sufficient supporting documentation must be provided to demonstrate meeting items a and b above.

The Ohio preference is for the sole purposes of evaluating and selecting vendor(s) for contract award and does not alter the vendors proposed pricing and firm rates. This preference will be applied to the proposed fees and may be used to select the winning vendor in the event that best value among multiple vendors are determined to be comparably equivalent best value by ODJFS.

Fees

Vendors are to provide proposed fees in the format provided and the fee table must be complete. Vendors are to use their professional comprehension of the effort required to propose an all-inclusive firm, fixed fee to implement the solutions and perform the services described in this RFQ. No separate travel expenses or any other type of reimbursable expenses will be paid under the contract that results from this RFQ. The fees offered in the quote response will be the prices in effect throughout the contract term, including any renewals of the contract.

Deliverable	Firm Fixed Fee
1. Project Plan	
2. Assess the current OUIO technology landscape and adjudication process and submit a comprehensive recommendation of refinements to the proposed solution and implementation plan.	
3. Testing*	
4. Go-live*	
Vendors may propose additional Deliverables in this table format	
Deliverables Total	

Maintenance and Operations (M&O)	Firm Fixed Fee
Annual M&O Year 1	
Annual M&O Year 2	
Annual M&O Year 3 (Optional)	
M&O Total	

Software Licensing (identify software name, number of licenses and license type)	Firm Fixed Fee

Software Licensing Total	

Cost Summary	Firm Fixed Fee
Deliverables Total	
M&O Total	
Software Licensing Total	
All Inclusive Firm Fixed Fee Total	

Please note: The Ohio Preference will be applied to the All-Inclusive Firm Fixed Fee Total for evaluation purposes only.

ATTACHMENT A

Non-Disclosure Agreement

This Non-Disclosure Agreement with the Ohio Department of Job and Family Services (ODJFS) is required because I may have access to confidential information as described in RFQ JFS-RFQ-2021-14-8185.

In connection with access to any and all ODJFS technical information referenced in this solicitation, I acknowledge and agree to abide by the following terms:

- I will access and use the technical information only as is necessary for the submission of a response to the solicitation and in compliance with the applicable provisions of federal and state confidentiality laws.
- I will store the technical information only on my employer's premises in an area that is physically safe from access by unauthorized persons during duty hours, as well as non-duty hours or when not in use.
- I will process the technical information and any records created from the information in a manner which will protect confidentiality and in such a way that unauthorized persons cannot retrieve the information by any means.
- I will properly dispose of technical information following submission of my response to the solicitation.
- I will immediately notify ODJFS Deputy Director of Contracts and Acquisitions of *any* suspected or actual violation of confidentiality.
- I have read and will comply with the terms, including but not limited to, the following: protecting the confidentiality of my personal access codes (e.g., username, password, etc.); securing computer equipment, disks and offices in which the confidential information may be kept; verifying that individuals requesting access to the information are authorized to receive them; and following procedures for the timely destruction of the information.
- I understand if I knowingly and intentionally violate any confidentiality terms or disclose confidential information, I may be subject to a fine and/or imprisonment under federal or State of Ohio laws.

By signing below, I acknowledge that I have read and understand the confidentiality requirements of ODJFS information, as well as the possible penalties for failure to comply, and will adhere to them.

Signature: ______________________________ Date: ______________

Printed Name: ______________________________

Company: ______________________________

ATTACHMENT B

AFFIRMATION AND DISCLOSURE FORM

By the signature affixed hereto, the Contractor affirms and understands that if awarded a contract, both the Contractor and any of its subcontractors shall perform no services requested under this Contract outside of the United States, nor allow State data to be sent, taken, accessed, tested, maintained, backed-up, stored or made available remotely (located) outside of the United States.

The Contractor shall provide all the name(s) and location(s) where services under this Contract will be performed and where data is located in the spaces provided below or by attachment. Failure to provide this information may result in no award. If the Contractor will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Principal location of business of Contractor:

   ______________________________ ______________________________
   (Address) (City, State, Zip)

   Name/Principal location of business of subcontractor(s):

   ______________________________ ______________________________
   (Name) (Address, City, State, Zip)

   ______________________________ ______________________________
   (Name) (Address, City, State, Zip)

2. Location where services will be performed by Contractor:

   ______________________________ ______________________________
   (Address) (City, State, Zip)

   Name/Location where services will be performed by subcontractor(s):

   ______________________________ ______________________________
   (Name) (Address, City, State, Zip)

(Name) (Address, City, State, Zip)

3. Location where state data will be located, by Contractor:

(Address) (City, State, Zip)

Name/Location(s) where state data will be located by subcontractor(s):

(Name) (Address, City, State, Zip)

(Name) (Address, City, State, Zip)

Contractor also affirms, understands and agrees that Contractor and its subcontractors are under a duty to disclose to the State any change or shift in location of services performed by Contractor or its subcontractors before, during and after execution of any Contract with the State. Contractor agrees it shall so notify the State immediately of any such change or shift in location of its services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Contractor to perform the services outside the United States.

On behalf of the Contractor, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure Form and have read and understand that this form is a part of any Contract that Contractor may enter into with the State and is incorporated therein.

By:

(Contractor)

Print Name: ___________________________

Title: ___________________________________

Date: ___________________________________

ATTACHMENT C

ODJFS Contract

Remainder of the page intentionally left blank

OHIO DEPARTMENT OF JOB AND FAMILY SERVICES
CONTRACT FOR SERVICES

C-2021-00-0000

RECITALS:

This Contract is entered into between the Ohio Department of Job and Family Services (ODJFS) and Vendor Name (CONTRACTOR).

A. ODJFS issued a Request for Proposals (RFP) titled ______, numbered ______, and dated [DATE], which is hereby incorporated by reference.

B. The ODJFS proposal review team recommended for award the Proposal of CONTRACTOR, submitted by CONTRACTOR by [Date] which is hereby incorporated by reference.

C. In the event of any inconsistency or ambiguity between the provisions of the RFP, the Proposal, or this Contract, the provisions of this Contract will determine the obligations of the parties. In the event that this Contract fails to clarify any inconsistency or ambiguity between the RFP and the Proposal, the RFP will determine the obligations of the parties. In the event of a disputed issue that is not addressed in any of the aforementioned documents, the parties hereby agree to make every reasonable effort to resolve the dispute in keeping with the objectives of this Contract and the budgetary and statutory constraints of ODJFS.

D. Key personnel that are identified by the CONTRACTOR as critical to the success of the Contract may not be removed without a reasonable notice to ODJFS, and replacements will not be made without ODJFS approval.

ARTICLE I. PURPOSE; DELIVERABLES

A. CONTRACTOR will perform its responsibilities (Deliverables) under this Contract as follows: OR CONTRACTOR will perform its responsibilities (Deliverables) under this Contract in accordance with the RFP and the Proposal. The Deliverables are summarized as follows:

B. The ODJFS Contract Manager is Name, or successor.

C. The ODJFS Contract Manager may periodically communicate specific requests and instructions to CONTRACTOR concerning the performance of the Deliverables described in this Contract. CONTRACTOR agrees to comply with any requests or instructions to the satisfaction of ODJFS within 10 business days after CONTRACTOR's receipt of the requests or instructions. ODJFS and CONTRACTOR expressly understand that any requests or instructions will be strictly to ensure the successful completion of the Deliverables described in this Contract, and are not intended to amend or alter this Contract in any way. If CONTRACTOR believes that any requests or instructions would materially alter the terms and conditions of this Contract or the compensation stated hereunder, CONTRACTOR will immediately notify ODJFS pursuant to the notice provisions of this Contract. CONTRACTOR agrees to consult with the ODJFS Contract Manager as necessary to ensure understanding of the Deliverables and the successful completion thereof.

D. **Ownership of Deliverables.**

1. All Deliverables provided by CONTRACTOR under this Contract or with funds hereunder, including any documents, data, photographs and negatives, electronic reports/records, or other media, are the property of ODJFS, which has an unrestricted right to reproduce, distribute, modify, maintain, and use the Deliverables. CONTRACTOR will not obtain copyright, patent, or other proprietary protection for the Deliverables. CONTRACTOR will not include in any Deliverable any copyrighted material, unless the copyright owner gives prior written approval for ODJFS and CONTRACTOR to use such copyrighted material in the manner provided herein. CONTRACTOR agrees that all Deliverables will be made freely available to the public unless ODJFS determines that, pursuant to state or federal law, such materials are confidential or otherwise exempted from disclosure.

2. All Deliverables provided or produced pursuant to this Contract will be considered "works made for hire" within the meaning of copyright laws of the United States and the State of Ohio. ODJFS is and will be deemed sole author of the Deliverables and sole owner of all rights therein. If any portion of the Deliverables is deemed not a "work made for hire," or if there are any rights in the Deliverables not conveyed to ODJFS, CONTRACTOR agrees to, and by executing this Contract does, assign ODJFS all worldwide rights, title, and interest in and to the Deliverables. ODJFS acknowledges that its sole ownership of the Deliverables under this Contract does not affect CONTRACTOR's right to use general concepts, algorithms, programming techniques, methodologies, or technology that CONTRACTOR developed prior to or as a result of this Contract or that are generally known and available.

3. CONTRACTOR understands that it must submit a written request to ODJFS and receive express written permission from ODJFS to include any of its own pre-existing, proprietary materials in any of the Deliverables under this Contract. ODJFS's approval of the inclusion of pre-existing, proprietary materials is predicated on CONTRACTOR granting to ODJFS and the State of Ohio a worldwide, non-exclusive, perpetual, royalty-free license to use, modify, sell, and otherwise distribute all such materials that are included in the Deliverables under this Contract. Upon request by CONTRACTOR, ODJFS will incorporate into any future copies of the Deliverables under this Contract any proprietary notice(s) CONTRACTOR may reasonably require for any pre-existing, proprietary materials included in the Deliverables of this Contract. Any proprietary notices will be the minimum required by law so as not to be seen as an endorsement by ODJFS or an advertisement for CONTRACTOR.

D. [UNIVERSITY RESEARCH] The Deliverables produced by CONTRACTOR under this Contract will be copyrighted in the name of CONTRACTOR. However, CONTRACTOR is required to obtain prior approval from ODJFS for release of any results, including preliminary and/or final results, related to funded projects or funded data under this Contract, and any documents, reports, data, photographs (including negatives), electronic reports and records, and other media under this Contract. CONTRACTOR hereby grants to ODJFS a perpetual, royalty free, non-exclusive, and irrevocable license to use, reproduce, publish, modify, and distribute any Deliverable either in whole or in part, and to produce derivative works. CONTRACTOR will assure that all products contain appropriate copyright attribution and ODJFS will treat Deliverable products as the intellectual property of CONTRACTOR for purposes of ORC 149.43. CONTRACTOR further reserves the right to use the Deliverables produced under this Contract for research and academic purposes, including the right to publish the work in scholarly journals or other academic publications.

ARTICLE II. EFFECTIVE DATE OF THE CONTRACT

A. This Contract is in effect from ____________ or the date of issuance of an approved State of Ohio purchase order, whichever is later, through ___________, unless this Contract is suspended or terminated prior to the expiration date.

B. It is expressly understood by both ODJFS and CONTRACTOR that this Contract will not be valid and enforceable until the Director of the Ohio Office of Budget and Management, first certifies, pursuant to Section 126.07 of the Ohio Revised Code (ORC), that there is a balance in the appropriation not already allocated to pay existing obligations. The ODJFS Contract Manager will notify CONTRACTOR when this certification is given.

ARTICLE III. COMPENSATION

A. The total amount payable under this Contract is TOTAL AMT and 00/100 Dollars ($TOTAL). ODJFS will pay an amount up to SFY1 AMT and 00/100 Dollars ($SFY 1) for State Fiscal Year (SFY) 2020, and up to SFY2 AMT and 00/100 Dollars ($SFY2) for SFY 2021, expressly for the completion of the Deliverables. CONTRACTOR understands that the terms of this Contract do not provide for compensation in excess of the total amount listed in this section. CONTRACTOR hereby waives the interest provisions of ORC 126.30.

B. It is further agreed that reimbursement of travel expenditures shall not exceed [SFY1 Travel Dollar Amount] and 00/100 Dollars ($SFY1 Travel) for SFY [SFY1] and [SFY2 Travel Dollar Amount] and 00/100 Dollars ($SFY2) for SFY [SFY2], which amount (s) is/are included in the total compensation figures above. Expense reimbursement authorized by this section is limited to actual and necessary expenses subject to the limits as established pursuant to ORC 126.31, which are set forth in OAC 126-1-02, as well as any other laws, regulations, or Governor's Executive Orders limiting travel expenses. CONTRACTOR expressly agrees not to submit claims for expenses which do not meet the requirements of this Section and further agrees to submit all claims to the ODJFS Contract Manager for approval prior to submitting a claim for reimbursement.

C. With the exception of travel expenses, line item expenses listed in the budget may be reallocated upon the written approval of the ODJFS Contract Manager as long as the total amounts per SFY and the total overall Contract amount remains unchanged. Any changes to the travel costs will require a written amendment to this Contract.

D. Compensation will be paid upon completion of the Deliverables pursuant to CONTRACTOR's accepted budget [or cost proposal] as incorporated below [or as attached].

E. CONTRACTOR will submit a detailed invoice(s) on a one-time, monthly, quarterly, annual basis to the ODJFS, Contract Manager, Office, Office Address OR Bureau of Accounts Payable at 30 East Broad Street, 37th Floor, Columbus, Ohio 43215. CONTRACTOR agrees to use an invoice instrument to be prescribed by ODJFS and will include in each invoice:

1. CONTRACTOR's name, complete address, and federal tax identification number;

2. Contract number and dates;

3. Purchase order number;

4. Amount and purpose of the invoice, including such detail as required per the compensation section of this Contract; Deliverables completed, description of services rendered, hourly rates and number of hours (if applicable), amount of monthly fee (if applicable), and itemized travel and other expenses if permitted by this Contract;

5. Description of Deliverables performed during the billing period; and

6. Other documentation requested by the ODJFS Contract Manager.

F. CONTRACTOR expressly understands that ODJFS will not compensate CONTRACTOR for any work performed prior to CONTRACTOR's receipt of notice from the ODJFS Contract Manager that the provisions of ORC 126.07 have been met as set forth in ARTICLE II, nor for work performed after the ending date of this Contract.

G. CONTRACTOR expressly understands that ODJFS does not have the ability to compensate CONTRACTOR for invoices submitted after the State of Ohio purchase order has been closed. State of Ohio purchase orders are issued per SFY. CONTRACTOR must submit final invoices for payment for each SFY no later than 90 calendar days after the end date of each SFY, or if earlier, the end date of this Contract. Failure to do so will be deemed a forfeiture of the remaining compensation due hereunder.

H. CONTRACTOR understands that availability of funds is contingent on appropriations made by the Ohio General Assembly or by funding sources external to the State of Ohio, such as federal funding. If the Ohio General Assembly or the external funding source fails at any time to continue funding ODJFS for the payments due under this Contract, this Contract will be terminated as of the date funding expires without further obligation of ODJFS or the State of Ohio.

I. CONTRACTOR and ODJFS understand that the terms of this Contract, when combined with any other payments made to or open encumbrances with CONTRACTOR during the same SFY, cannot establish compensation in excess of Fifty Thousand and 00/100 Dollars ($50,000.00) aggregate without prior approval from the State Controlling Board in accordance with ORC 127.16.

ARTICLE IV. SUSPENSION AND TERMINATION, BREACH AND DEFAULT

A. This Contract will automatically terminate upon expiration of the time period in ARTICLE II, or upon completion of all Deliverables, or once all compensation has been paid.

B. Notwithstanding other provisions in this ARTICLE, either party may terminate this Contract at will by giving 30 calendar days written notice to the other party. Upon written notice to CONTRACTOR, ODJFS may immediately suspend this Contract at ODJFS's sole discretion.

C. Notwithstanding the provisions of Sections A or B, above, ODJFS may suspend or terminate this Contract immediately upon delivery of a written notice to CONTRACTOR if:

1. ODJFS loses funding as described in ARTICLE III;

2. ODJFS discovers any illegal conduct by CONTRACTOR; or

3. CONTRACTOR has violated any provision of ARTICLE VIII.

Suspension or termination under this provision shall not entitle CONTRACTOR to any rights or remedies described in Section F of this ARTICLE.

D. Unless otherwise provided for in this ARTICLE, CONTRACTOR will have 30 calendar days within which to cure any breach that is curable after receipt of written notice from ODJFS that CONTRACTOR is in breach of any of its obligations under this Contract. If CONTRACTOR fails to cure the breach within the 30 calendar days after written notice or if the breach is not curable, ODJFS may immediately suspend or terminate this Contract. ODJFS may also suspend or terminate this Contract when breaches are persistent, regardless of whether they are cured within 30 calendar days. For purposes of this Section, "persistent" means that ODJFS has notified CONTRACTOR two times in writing of CONTRACTOR's failure to meet any of its contractual obligations. The two notices do not have to relate to the same obligation or type of failure. After the second notice, ODJFS may suspend or terminate this Contract without a cure period if CONTRACTOR again fails to meet any contractual obligation. At the sole discretion of ODJFS, certain instances of breach may require a shorter cure period than the 30 calendar days generally applicable in this Section. In such instances, ODJFS will include in its notice of breach the shorter cure period deemed appropriate. If ODJFS does not give timely notice of a breach to CONTRACTOR, ODJFS has not waived any of its rights or remedies concerning the breach.

E. CONTRACTOR, upon receiving notice of suspension or termination, will:

1. Cease performance of the suspended or terminated Deliverables;

2. Take all necessary steps to limit disbursements and minimize costs including, but not limited to, suspending or terminating all contracts and subgrants related to suspended or terminated Deliverables and refusing any additional orders;

3. Prepare and furnish a report to ODJFS, as of the date the notice of termination or suspension was received, that describes the status and percentage of completion of all Deliverables, including the results accomplished and the conclusions reached through Deliverables;

4. Deliver all records in their native format relating to cost, work performed, supporting documentation for invoices submitted to ODJFS, and deliver any and all materials or work produced under or pertaining to this Contract whether completed or not; and

5. Perform any other tasks ODJFS requires.

F. In the event of suspension or termination under this ARTICLE, ODJFS will, upon receipt of a proper invoice from CONTRACTOR, determine the amount of any unpaid Contract funds due to CONTRACTOR for Deliverables performed before CONTRACTOR received notice of termination or suspension. In order to determine the amount due to CONTRACTOR, ODJFS will base its calculations on the payment method described in ARTICLE III and any funds previously paid by or on behalf of ODJFS. ODJFS will not be liable for any further claims submitted by CONTRACTOR.

G. If ODJFS terminates this Contract for any reason provided in this ARTICLE, except for termination at will pursuant to Section B or termination for loss of funding pursuant to Section C, ODJFS will be entitled to utilize another contractor to complete the Deliverables of this Contract on any commercially reasonable terms as ODJFS and the covering contractor may agree. In this event, CONTRACTOR will be liable to ODJFS for all costs related to covering the project to the extent that such costs, when combined with payments already made to CONTRACTOR prior to termination, exceed the costs that ODJFS would have incurred under this Contract. CONTRACTOR's liability under this Section is in addition to any other remedies available to ODJFS pursuant to this Contract.

H. Upon CONTRACTOR's breach or default of provisions, obligations, or duties embodied in this Contract or any term of an award, a federal statute or regulation, an assurance, a State plan or application, a notice of award, or other applicable rule, ODJFS reserves the right to exercise any administrative, contractual, equitable, or legal remedies available without limitation. Any waiver by ODJFS of an occurrence of breach or default is not a waiver of subsequent occurrences. If ODJFS or CONTRACTOR fails to perform any obligation under this Contract and the other party subsequently waives the failure, the waiver will be limited to that particular occurrence of a failure and will not be deemed to waive other failures that may occur. Waiver by ODJFS will not be effective unless it is in writing signed by the ODJFS Director.

ARTICLE V. NOTICES

A. ODJFS and CONTRACTOR agree that communication regarding Deliverables, scope of work, invoice or billing questions, or other routine instructions will be between CONTRACTOR and the identified ODJFS Contract Manager.

B. Notices to ODJFS from CONTRACTOR that concern changes to CONTRACTOR's principal place of operation, billing address, legal name, federal tax identification number, mergers or acquisitions, corporate form, excusable delay, termination, bankruptcy, assignment, any notice pursuant to ARTICLE VIII, and/or any other formal notice regarding this Contract will be sent to the ODJFS Deputy Director of Contracts and Acquisitions at 30 East Broad Street, 31st Floor, Columbus, Ohio 43215.

C. Notices to CONTRACTOR from ODJFS concerning termination, suspension, option to renew, breach, default, or other formal notices regarding this Contract will be sent to CONTRACTOR's representative at the address appearing on the signature page of this Contract.

D. All notices will be in writing and will be deemed given when received. All notices must be sent using a delivery method that documents actual delivery to the appropriate address herein indicated (*e.g.*, registered or certified mail, postage prepaid).

ARTICLE VI. RECORDS, DOCUMENTS AND INFORMATION

CONTRACTOR agrees that all records, documents, writings, and other information, created or used pursuant to this Contract will be treated according to the following terms, and that the terms will be included in any subcontract agreements executed for the performance of the Deliverables under this Contract:

A. CONTRACTOR agrees that any media produced pursuant to this Contract or acquired with Contract funds will become the property of ODJFS. This includes all documents, reports, data, photographs (including negatives), and electronic reports and records. ODJFS will maintain the unrestricted right to reproduce, distribute, modify, maintain, and use the media in any way ODJFS deems appropriate. CONTRACTOR further agrees not to seek or obtain copyright, patent or other proprietary protection for any materials or items produced under this Contract. CONTRACTOR understands that all materials and items produced under this Contract will be made freely available to the public unless ODJFS determines that certain materials are confidential under federal or state law.

A. [UNIVERSITY] ODJFS agrees that any media (including documents, reports, data, photographs, negatives, electronic reports and records) produced pursuant to this Contract or acquired with Contract funds will become the property of CONTRACTOR; however, CONTRACTOR hereby grants to ODJFS a perpetual, royalty free, non-exclusive, and irrevocable license to use, reproduce, publish, modify, and distribute any such media. CONTRACTOR will assure that all products contain appropriate copyright attribution and ODJFS will treat Deliverable products that contain appropriate copyright attribution as the intellectual property of CONTRACTOR for purposes of ORC 149.43.

B. All ODJFS information that is classified as public or private under Ohio law will be treated as such by CONTRACTOR. Should the nature of any information be in question, ODJFS will determine whether the information is public or private. CONTRACTOR will restrict the use of any information, systems, or records

ODJFS provides to the specific Deliverables of this Contract. CONTRACTOR and its employees agree to be bound by the same standards and rules of confidentiality that apply to employees of ODJFS and the State of Ohio. CONTRACTOR agrees that the terms of this section will be included in any subcontract executed by CONTRACTOR for work under this Contract.

C. CONTRACTOR information that is proprietary and has been specifically identified by CONTRACTOR as proprietary will be held as confidential by ODJFS. Proprietary information is information that would put CONTRACTOR at a competitive disadvantage in CONTRACTOR's market place and trade if it were made public. ODJFS reserves the right to require reasonable evidence of CONTRACTOR's assertion of the proprietary nature of any information. The provisions of this ARTICLE are not self-executing. CONTRACTOR must demonstrate that any information claimed as proprietary meets the definition of "trade secret" found at ORC 1333.61. CONTRACTOR will defend such a claim.

D. For Audit Purposes Only: All records relating to cost, work performed, supporting documentation for invoices submitted to ODJFS, and copies of all materials produced under or pertaining to this Contract will be retained by CONTRACTOR and will be made available for audit by state and federal government entities that include but are not limited to, ODJFS, the Ohio Auditor of State, the Ohio Inspector General and all duly authorized law enforcement officials. The records and materials will be retained and made available for a minimum of three years after CONTRACTOR receives the last payment pursuant to this Contract. If an audit, litigation or similar action is initiated during this time period, CONTRACTOR will retain the records until the action is concluded and all issues are resolved, or until the end of the three-year period if the action is resolved prior to the end of the three-year period. If applicable, CONTRACTOR must meet the requirements of the federal Office of Management and Budget (OMB) Omni-Circular, Title 2 of the Code of Federal Regulations (CFR) Part 200. CONTRACTOR acknowledges, in accordance with ORC 149.43, that financial records related to the performance of services under this Contract are presumptively deemed public records.

E. All records relating to cost, work performed, supporting documentation for invoices submitted to ODJFS, and copies of all materials produced under or pertaining to this Contract will be retained by CONTRACTOR in accordance to the appropriate records retention schedule. The appropriate records retention schedule for this Contract is INSERT RECORDS SCHEDULE [Must be minimum of three years, 2 CFR 200.333]. If any records are destroyed prior to the date as determined by the appropriate records retention schedule, CONTRACTOR agrees to pay all costs associated with any cause, action or litigation arising from such destruction.

F. CONTRACTOR agrees to retain all records in accordance with any litigation holds that are provided to them by ODJFS, and actively participate in the discovery process if required to do so, at no additional charge. Litigation holds may require CONTRACTOR to keep the records longer than the approved records retention schedule. CONTRACTOR will be notified by ODJFS when the litigation hold ends and retention can resume based on the approved records retention schedule. If CONTRACTOR fails to retain the pertinent records after receiving a litigation hold from ODJFS, CONTRACTOR agrees to pay all costs, damages and expenses associated with any cause, action or litigation arising from such destruction.

G. If applicable, CONTRACTOR hereby agrees to current and ongoing compliance with Title 42, Sections 1320d through 1320d-8 of the United States Code (42 USC 1320d-1320d-8) and the implementing regulations found at 45 CFR 164.502(e) and 164.504(e) regarding disclosure of Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If applicable, CONTRACTOR further agrees to include the terms of this section in any subcontracts that may be executed pursuant to this Contract.

ARTICLE VII. AMENDMENT AND ASSIGNMENT

A. This writing constitutes the entire agreement between ODJFS and CONTRACTOR with respect to all matters herein. Only a writing signed by both parties may amend this Contract. However, ODJFS and CONTRACTOR agree that any amendments to any laws or regulations cited herein will result in the correlative modification of this Contract without the necessity for executing written amendments. It is agreed that line item budget modifications may be made, in writing, upon approval by the ODJFS Contract Manager without a written amendment pursuant to ARTICLE III. Any written amendment to this Contract will be prospective in nature.

B. CONTRACTOR agrees not to assign any interest in this Contract nor transfer any interest in the Contract without the prior written approval of ODJFS. CONTRACTOR will submit any requests for approval of assignments and transfers to the ODJFS Contract Manager at least 10 business days prior to the desired effective date. CONTRACTOR understands that any assignments and transfers will be subject to any conditions ODJFS deems necessary and that no approval by ODJFS will be deemed to provide for any ODJFS obligation that exceeds the Contract amount specified in ARTICLE III of this Contract.

ARTICLE VIII. CONTRACTOR CERTIFICATION OF COMPLIANCE WITH SPECIAL CONDITIONS

By accepting this Contract and by executing this Contract, CONTRACTOR hereby affirms current and continued compliance with each condition listed in this ARTICLE. CONTRACTOR's certification of compliance with each of these conditions is considered a material representation of fact upon which ODJFS relied in entering into this Contract:

A. If at any time, CONTRACTOR is not in compliance with the conditions affirmed in this Section, ODJFS will consider this Contract *void ab initio* and will deliver written notice to CONTRACTOR. Any funds the State of Ohio paid CONTRACTOR for work performed before CONTRACTOR received notice that the Contract is *void ab initio* will be immediately repaid or the State of Ohio may commence an action for recovery against CONTRACTOR.

1. **Federal Debarment Requirements.** CONTRACTOR affirms that neither CONTRACTOR nor any of its principals or subcontractors, is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by any federal agency. CONTRACTOR also affirms that within three years preceding this Contract neither CONTRACTOR nor any of its principals:

a. Have been convicted of, or had a civil judgment rendered against them for commission of fraud or other criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state, or local public transaction or contract under a public transaction; for violation of federal or state antitrust statutes; for commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements; or for receiving stolen property; or

b. Are presently indicted or otherwise criminally or civilly charged by a government entity (Federal, State, or local) for the commission of any of the offenses listed in this paragraph and have not had any federal, state, or local, public transactions terminated for cause or default.

2. **Qualifications to Conduct Business.** CONTRACTOR affirms that it has all of the approvals, licenses, or other qualifications needed to conduct business in Ohio and all are current. If at any time during the Contract period CONTRACTOR, for any reason, becomes disqualified from conducting business in the State of Ohio, CONTRACTOR will immediately notify ODJFS in writing and will immediately cease performance of all Deliverables.

3. **Unfair Labor Practices.** CONTRACTOR affirms that neither CONTRACTOR nor its principals are on the most recent list established by the Ohio Secretary of State, pursuant to ORC 121.23, which would identify CONTRACTOR as having more than one unfair labor practice contempt of court finding.

4. **Finding for Recovery.** CONTRACTOR affirms that neither CONTRACTOR nor its principals or subcontractors, is subject to a finding for recovery under ORC 9.24, or it has taken the appropriate remedial steps required, or otherwise qualifies under ORC 9.24 to contract with the State of Ohio.

B. If at any time CONTRACTOR is not in compliance with the conditions affirmed in this Section, ODJFS may immediately suspend or terminate this Contract and will deliver written notice to CONTRACTOR. CONTRACTOR will be entitled to compensation, upon submission of a proper invoice per ARTICLE III, only for work performed during the time CONTRACTOR was in compliance with the provisions of this Section. Any funds paid by the State of Ohio for work performed during a period when CONTRACTOR was not in compliance with this Section will be immediately repaid or the State of Ohio may commence an action for recovery against CONTRACTOR.

1. **Americans with Disabilities.** CONTRACTOR, its officers, employees, members, and subcontractors hereby affirm current and ongoing compliance with all statutes and regulations

pertaining to The Americans with Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973.

2. **Fair Labor Standards and Employment Practices**.

a. CONTRACTOR certifies that it is in compliance with all applicable federal and state laws, rules, and regulations governing fair labor and employment practices, including ORC 125.111 and all related Executive Orders.

b. In carrying out this Contract, CONTRACTOR will not discriminate against any employee or applicant for employment because of race, color, religion, gender, national origin, ancestry, military status, disability, age, genetic information, or sexual orientation, in making any of the following employment decisions: hiring, layoff, termination, transfer, promotion, demotion, rate of compensation, and eligibility for in-service training programs.

c. CONTRACTOR agrees to post notices affirming compliance with all applicable federal and state non-discrimination laws in conspicuous places accessible to all employees and applicants for employment.

d. If applicable, CONTRACTOR agrees to comply with the provisions of Equal Employment Opportunity Clause (41 CFR Part 60), the Davis-Bacon Act (40 USC 3141-3148), the Copeland Act (40 USC 3145), and the Contract Work Hours and Safety Standards Act (40 USC Chapter 37), regarding labor standards for federally assisted construction contracts. If applicable, CONTRACTOR agrees to comply with ORC Chapter 4115 and corresponding Ohio Administrative Code rules.

e. CONTRACTOR will incorporate the foregoing requirements of this Paragraph 2 in all of its subgrants or subcontracts for any of the work prescribed herein.

3. **Ethics and Conflicts of Interest Laws**.

a. CONTRACTOR certifies that by executing this Contract, it has reviewed, knows and understands the State of Ohio's ethics and conflict of interest laws. CONTRACTOR further agrees that it will not engage in any action(s) inconsistent with Ohio ethics laws or any Executive Orders.

b. CONTRACTOR certifies, by executing this Contract, that no party who holds a position listed or described in ORC 3517.13 (I) or (J), has made, while in his/her current position, one or more personal monetary contributions in excess of One Thousand and 00/100 Dollars ($1,000.00) to the current Governor or to the Governor's campaign committee when he was a candidate for office, within the previous two calendar years.

c. CONTRACTOR agrees to refrain from promising or giving to any ODJFS employee anything of value that could be construed as having a substantial and improper influence upon the employee with respect to the employee's duties. CONTRACTOR further agrees that it will not solicit any ODJFS employee to violate ORC 102.03, 2921.42, or 2921.43.

d. CONTRACTOR agrees that CONTRACTOR, its officers, employees, and members have not nor will they acquire any interest, whether personal, business, direct or indirect, that is incompatible, in conflict with, or would compromise the discharge and fulfillment of CONTRACTOR's functions and responsibilities under this Contract. If CONTRACTOR, its officers, employees, or members acquire any incompatible, conflicting, or compromising interest, CONTRACTOR agrees it will immediately disclose the interest in writing to the ODJFS Chief Legal Counsel at 30 East Broad Street, 31st Floor, Columbus, Ohio 43215. CONTRACTOR further agrees that the person with the conflicting interest will not participate in any Deliverables until ODJFS determines that participation would not be contrary to public interest.

4. **Lobbying Restrictions.**

   a. CONTRACTOR affirms that no federal funds paid to CONTRACTOR by ODJFS through this Contract or any other agreement have been or will be used to lobby Congress or any federal agency in connection with a particular contract, grant, cooperative agreement or loan. CONTRACTOR further affirms compliance with all federal lobbying restrictions, including 31 USC 1352. If this Contract exceeds One Hundred Thousand and 00/100 Dollars ($100,000.00), CONTRACTOR affirms that it has executed and filed the Disclosure of Lobbying Activities standard form LLL, if required by federal regulations, and is in compliance with 31 USC 1352 the Byrd anti-lobbying amendment.

   b. CONTRACTOR certifies compliance with the Ohio executive agency lobbying restrictions contained in ORC 121.60 to 121.69.

5. **Child Support Enforcement.** CONTRACTOR agrees to cooperate with ODJFS and any child support enforcement agency in ensuring that CONTRACTOR and its employees meet child support obligations established by state and federal law including present and future compliance with any court or valid administrative order for the withholding of support issued pursuant to the applicable sections of ORC Chapters 3119, 3121, 3123, and 3125.

6. **Pro-Child Act.** If any Deliverables call for services to minors, CONTRACTOR agrees to comply with the Pro-Children Act of 1994; Public Law 103-277, Part C – Environment Tobacco Smoke that requires smoking to be banned in any portion of any indoor facility owned, leased, or contracted by an entity that will routinely or regularly use the facility for the provision of health care services, day care, library services, or education to children under the age of 18.

7. **Drug-Free Workplace**. CONTRACTOR, its officers, employees, members, any subcontractors and/or any independent contractors (including all field staff) associated with this Contract agree to comply with all applicable state and federal laws, including, but not limited to, 41 USC Chapter 10 and 2 CFR 182, regarding a drug-free workplace. CONTRACTOR will make a good faith effort to ensure that none of CONTRACTOR's officers, employees, members, or subgrantees will purchase, transfer, use, or possess illegal drugs or alcohol or abuse prescription drugs in any way while working or while on public property.

8. **Work Programs.** CONTRACTOR agrees not to discriminate against individuals who have or are participating in any work program administered by any county department of Job and Family Services under ORC Chapter 5101 or 5107.

9. **MBE/EDGE.** Pursuant to the Governor’s Executive Order 2008-13S, CONTRACTOR agrees to purchase goods and services under this Contract from certified Minority Business Enterprise (MBE) and Encouraging Diversity, Growth, and Equity (EDGE) vendors whenever possible. CONTRACTOR agrees to encourage any of its subgrantees or subcontractors to purchase goods and services from certified MBE and EDGE vendors. In accordance with 2 CFR 200.321, CONTRACTOR agrees to take affirmative steps to assure that minority businesses, women’s business enterprises and labor surplus area firms are used when possible.

10. **Expenditure of Public Funds for Offshore Services—Executive Order Requirements.**

    [PUBLIC UNIVERSITY] CONTRACTOR, a public university, certifies that by executing this Contract, it has reviewed and understands ODJFS’s obligation under Governor’s Executive Order 2019-12D, and will perform no services required under this Contract outside of the United States. [delete a-d]

    a. CONTRACTOR certifies that by executing this Contract, it has reviewed, understands, and will abide by the Governor’s Executive Order 2019-12D and shall abide by those requirements in the performance of this Contract, and shall perform no services required under this Contract outside of the United States.

    b. Prior to performing any services, and when there is a change in the location of any services provided under this Contract, CONTRACTOR must disclose:

(1) The location(s) where all services will be performed by CONTRACTOR or any subcontractor;

(2) The location(s) where any state data associated with any of the services through this Contract will be accessed, tested, maintained, backed-up, or stored; and

(3) The principal location of business for the contractor and all subcontractors.

c. CONTRACTOR also affirms, understands, and agrees to immediately notify ODJFS of any change or shift in the location(s) of services performed by CONTRACTOR or its subcontractors under this Contract, and no services shall be changed or shifted to a location outside of the United States.

d. Termination, Sanction, Damages**:** ODJFS is not obligated and shall not pay for any services provided under this Contract that CONTRACTOR or any of its subcontractors performed outside of the United States. If services are performed outside of the United States, this will be treated as a material breach of the Contract, and CONTRACTOR shall immediately return to ODJFS all funds paid for those services.

In addition, if CONTRACTOR or any of its subcontractors perform any such services outside of the United States, ODJFS may, at any time after the breach, terminate this Contract for such breach, upon written notice to CONTRACTOR. If ODJFS terminates the Contract, ODJFS may buy substitute services from a third party, and may recover the additional costs associated with acquiring the substitute services.

11. [REMOVE IF STATE FUNDS ONLY] [PRIVATE ENTITY] **Combating Trafficking in Persons.**

a. CONTRACTOR agrees that it is in compliance with the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 USC 7104), *see* 2 CFR Part 175 and the Federal Acquisition Regulation (FAR) for Combating Trafficking in Persons, 48 CFR Subpart 22.17. The provisions found in 48 CFR Subpart 52.222-50 are hereby incorporated into this Contract by reference.

b. CONTRACTOR, its employees, its subcontractors, or subcontractor's employees are prohibited from: engaging in severe forms of trafficking in persons during the period of performance of the Contract; procuring commercial sex acts during the period of performance of the Contract; or using forced labor in the performance of the Contract.

c. CONTRACTOR agrees that it shall notify its employees, and require all of its subcontractors to notify their employees, of the prohibited activities described in the preceding paragraph.

d. ODJFS has the right to immediately and unilaterally terminate this Contract if any provision in this Section is violated and ODJFS may implement section 106(g) of the TVPA, *see* 2 CFR 175.10.

11. [REMOVE IF STATE FUNDS ONLY] [PUBLIC UNIVERSITY/PUBLIC ENTITY] **Combating Trafficking in Persons.** Pursuant to 22 USC 7104(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 USC 7104), *see* 2 CFR Part 175, this Contract may be terminated without penalty if CONTRACTOR or any subcontractor paid with Contract funds:

a. Engages in severe forms of trafficking in persons or has procured a commercial sex act during the period of time this Contract or any subcontracts or subagreements are in effect; or

b. Uses forced labor in the performance of activities under this Contract or under any subcontracts or subagreements.

c. CONTRACTOR agrees that it shall notify, and require all of its subcontractors to notify, its employees of the prohibited activities described in the preceding paragraph.

d. ODJFS has the right to immediately and unilaterally terminate this Contract if any provision in this Section is violated and ODJFS may implement section 106(g) of the TVPA, *see* 2 CFR 175.10.

12. **Civil Rights Assurance.** The CONTRACTOR hereby agrees that it will comply with Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq.) and the Age Discrimination Act of 1975 (42 U.S.C. § 6101 et seq.).

13. [REMOVE IF STATE FUNDS ONLY] **Clean Air Act and Federal Water Pollution Control Act**. CONTRACTOR agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Regional Office of the United States Environmental Protection Agency (USEPA) and ODJFS.

14. [REMOVE IF STATE FUNDS ONLY] **Procuring Recovered Materials.** CONTRACTOR agrees to comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the USEPA at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding federal fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the USEPA guidelines.

15. [REMOVE IF STATE FUNDS ONLY] **Rights to Inventions.** If applicable, if any products or services under this Contract meet the definition of "funding agreement" under 37 CFR 401.2(a), and CONTRACTOR enters into a subcontract or subgrant with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that funding agreement, the Contractor must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any applicable federal and state regulations.

16. [FOR PROFIT ORGANIZATION] **Boycotting**. Pursuant to Division B of ORC 9.76, the CONTRACTOR warrants that it is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the contract period.

17. **Certification of Compliance.** CONTRACTOR certifies that it is in compliance with all other applicable federal and state, local laws, regulations, rules, and Executive Orders and will require the same certification from its subgrantees or subcontractors.

ARTICLE IX. MISCELLANEOUS PROVISIONS

A. **Independent Contractor.** CONTRACTOR agrees that no agency, employment, joint venture, or partnership has been or will be created between ODJFS and CONTRACTOR. CONTRACTOR further agrees that as an independent contractor, it assumes all responsibility for any federal, state, municipal or other tax liabilities along with workers compensation, unemployment compensation and insurance premiums that may accrue as a result of funds received pursuant to this Contract. CONTRACTOR agrees that it is an independent contractor for all purposes including, but not limited to, the application of the Fair Labor Standards Act, the Social Security Act, the Federal Unemployment Tax Act, the Federal Insurance Contribution Act, provisions of the Internal Revenue Code, Ohio tax law, Workers Compensation law, and Unemployment Insurance law. CONTRACTOR acknowledges and agrees any individual providing personal services under this Contract is not a public employee for the purposes of Chapter 145 of the Revised Code. Pursuant to ORC 145.038, ODJFS is required to provide individuals and business entities with fewer than five employees the Independent Contractor Acknowledgment (Form PEDACKN), please see Attachment A. This form requires CONTRACTOR to acknowledge that ODJFS has notified CONTRACTOR that he or she has not been classified as a public employee and no OPERS contributions will be made on his or her behalf for these services. If CONTRACTOR is a business entity with fewer than five employees, please have each employee complete the PEDACKN form, the first two pages of Attachment A. If CONTRACTOR is not an individual or a business entity with fewer than five employees, please complete page three of Attachment A.

B. **Liability.** To the extent allowable by law, CONTRACTOR agrees to hold ODJFS harmless in any and all claims for personal injury, property damage, infringement resulting, and/or any other claims arising from the performance of the Deliverables. CONTRACTOR's sole and exclusive remedy for any ODJFS failure to perform under this Contract will be an action in the Ohio Court of Claims pursuant to ORC Chapter 2743 that will be subject to the limitations set forth in this ARTICLE. In no event will ODJFS be liable for any indirect or consequential damages, including loss of profits, even if ODJFS knew or should have known of the possibility of such damages. To the extent that ODJFS is a party to any litigation arising out of or relating in any way to this Contract or the performance thereunder, such an action shall be brought only in a court of competent jurisdiction in Franklin County, Ohio.

B. [PUBLIC UNIVERSITY/PUBLIC ENTITY] **Limitation of Liability.** Each party agrees to be responsible for any of its own negligent acts or omissions or those of its agent, employees, or subcontractors. Each party further agrees to be responsible for its own defense and any judgments and costs that may arise from such negligent acts or omissions. Nothing in this Contract will impute or transfer any such liability or responsibility from one party to the other. To the maximum extent permitted by law, the parties' liability for damages, whether in contract or in tort, may not exceed the total amount of compensation payable to CONTRACTOR under ARTICLE III or the actual amount of direct damages incurred by any party whichever is less. CONTRACTOR's sole and exclusive remedy for ODJFS's failure to perform under this Contract is an action in the Ohio Court of Claims, pursuant to ORC Chapter 2743, and subject to the limitations set forth in this ARTICLE. In no event will either party be liable for any indirect or consequential damages, including loss of profits, even if a party knew or should have known of the possibility of such damages.

C. **Infringement of Patent or Copyright.** To the extent allowable by law and subject to ORC 109.02, CONTRACTOR agrees to defend any suit or proceeding brought against ODJFS, any official or employee of ODJFS acting in his or her official capacity, or the State of Ohio due to any alleged infringement of patent or copyright arising out of the performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by CONTRACTOR. ODJFS will provide prompt notification in writing of such suit or proceeding; full right, authorization, and opportunity to conduct the defense thereof; and full disclosure of information along with all reasonable cooperation for the defense of the suit. ODJFS may participate in the defense of any such action. CONTRACTOR agrees to pay all damages and costs awarded against ODJFS, any official or employee of ODJFS in his or her official capacity, or the State of Ohio as a result of any suit or proceeding referred to in this Section C. If any information and/or assistance is furnished by ODJFS at CONTRACTOR's written request, it is at CONTRACTOR's expense. If any of the materials, reports, or studies provided by CONTRACTOR are found to be infringing items and the use or publication thereof is enjoined, CONTRACTOR agrees to, at its own expense and at its option, either procure the right to publish or continue use of such infringing materials, reports, or studies; replace them with non-infringing items of equivalent value; or modify them so that they are no longer infringing. The obligations of CONTRACTOR under this Section survive the termination of this Contract, without limitation.

C. [PUBLIC UNIVERSITY/PUBLIC ENTITY **Infringement of Patent or Copyright.** To the extent permitted by law, if any of the materials, reports, or studies provided by CONTRACTOR are found to be infringing items and the use or publication thereof is enjoined, CONTRACTOR agrees to, at its own expense and at its option, either procure the right to publish or continue use of such infringing materials, reports, or studies; replace them with non-infringing items of equivalent value; or modify them so that they are no longer infringing. The obligations of CONTRACTOR under this Section survive the termination of this Contract, without limitation.

D. **Liens.** CONTRACTOR will not permit any lien or claim to be filed or prosecuted against ODJFS or the State of Ohio because of any labor, services, or materials furnished. If CONTRACTOR fails, neglects, or refuses to make prompt payment of any claims for labor, services, or materials furnished to CONTRACTOR in connection with this Contract, ODJFS or the State of Ohio may, but is not obligated to, pay those claims and charge the amount of payment against the funds due or to become due to CONTRACTOR under this Contract.

E. **Delay.** Neither party will be liable for any delay in its performance that arises from causes beyond its control and without its negligence or fault. The delaying party will notify the other promptly of any material delay in performance and will specify in writing the proposed revised performance date as soon as practicable after notice of delay. The delaying party must also describe the cause of the delay and its proposal to remove or mitigate the delay. Notices will be sent pursuant to ARTICLE V. In the event of excusable delay, the date of performance or delivery of products may be extended by amendment, if applicable, for a time period equal to that lost due to the excusable delay. Reliance on a claim of excusable delay may only be asserted if the delaying party has taken commercially reasonable steps to mitigate or avoid the delay. Items that are controllable by CONTRACTOR's subcontractor(s) will be considered controllable by CONTRACTOR, except for third-party manufacturers supplying commercial items and over whom CONTRACTOR has no legal control. The final determination of whether an instance of delay is excusable lies with ODJFS in its discretion.

F. **Insurance**. CONTRACTOR agrees to maintain, at its own cost, automobile, fleet, and commercial general liability insurance.

G. **Attachments.** Attachments and documents referenced in this Contract are made a part hereof, and are incorporated as terms and conditions of this Contract. In the event a conflict of terms, the terms and conditions of this Contract shall take precedence over any conflicting terms.

H. **Counterpart**. This Contract may be executed in one, or more than one counterpart and each executed counterpart shall be considered an original, provided that such counterpart is delivered to the other party by facsimile, mail courier or electronic mail, all of which together shall constitute one and the same agreement.

ARTICLE X. CONSTRUCTION

This Contract will be governed, construed, and enforced in accordance with the laws of the State of Ohio. Should any portion of this Contract be found unenforceable by operation of statute or by administrative or judicial decision, the remaining portions of this Contract will not be affected as long as the absence of the illegal or unenforceable provision does not render the performance of the remainder of the Contract impossible.

Signature Page Follows:

Remainder of page intentionally left blank

OHIO DEPARTMENT OF JOB AND FAMILY SERVICES
CONTRACT FOR SERVICES

SIGNATURE PAGE

C-2021-00-0000

THE PARTIES HAVE EXECUTED THIS CONTRACT AGREEMENT AS OF THE DATE OF THE SIGNATURE OF THE DIRECTOR OF THE OHIO DEPARTMENT OF JOB AND FAMILY SERVICES.

Vendor Name	Ohio Department of Job and Family Services
______________________________ Authorized Signature (Blue Ink Please)	______________________________ Kimberly L. Hall, Director
______________________________ Printed Name	______________________________ Date
______________________________ Date	
Address City, State, Zip	30 East Broad Street, 32nd Floor Columbus, Ohio 43215

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.

Contents

1. Overview of Supplement

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 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.

Please note that 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 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.

2. 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 IT Policies, Standards, IT Bulletins and DAS Polices

Item	Link
State of Ohio IT Policies	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Policies
State of Ohio IT Standards	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards
State of Ohio IT Bulletins	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Bulletins
DAS Policies	100-11 Protecting Privacy 100-12 ID Badges & Visitors Policy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series https://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies

3. State IT Service Requirements

3.1. Requirements Overview

Contractors performing the work under the Contract are required to comply with the standards and leverage State IT services outlined in this document unless the State has approved a variance. See note above in Section 1 regarding instructions to propose variances to the requirements outlined in this supplement.

3.2. Solution Architecture Requirements

Unless stipulated otherwise in the RFP, on premise or cloud-based solutions are permitted by the State. Custom or unique built solutions must comply with State requirements including using the State's virtualized computing platform (State Private Cloud) or the State of Ohio Enterprise brokered public cloud service and running on databases that comply with the State's supported database platforms. Custom or unique built solutions are required to include installation of third-party applications on State provided computing platforms which could be on the State-run private cloud or the State-run public cloud. Dedicated server platforms are not compliant with the State's virtualization requirements. The State provides different storage pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads. Custom or unique built solutions must take advantage of the State's storage service offerings.

Custom or unique built solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.). Applications must be developed with standards-based open application programming interfaces and all available features and functionality accessible via APIs must be disclosed in the proposed solution. Custom or unique built solutions with Open APIs proposed must include periodic updates throughout the project lifecycle and a final update as part of the closure phase.

Cloud-based solutions must utilize as many platform services as possible and comply with State requirements to run in the State of Ohio Enterprise brokered public cloud service. Currently, Microsoft Azure and Amazon Web Services are hosted by DAS OIT for the State of Ohio.

3.3. State of Ohio IT Services

The Department of Administrative Services Office of Information Technology (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. This document 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.

3.3.1. 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.

3.3.1.1. 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 an authorization layer and allows for the integration and extension of InnovateOhio Platform identity services into applications. Customizable to User needs.

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

3.3.1.2. 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
- Mobile Ready
- 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

3.3.1.3. Analytics and Data Sharing Products

Applied Analytics
Ohio's applied analytics solution 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. From ideation and solution design to data science and engineering, the applied analytics solution enables the User to move from concept to results.

- Advanced Data Science
- Data Strategy Optimization
- Ideation & Scoping
- Solution Design
- Visual Data Discovery
- Workflow Integration

Big Data Platform
Ohio's data sharing and analytics platform provides public/private cloud deployment models that are secure, flexible, and scalable, powering analytics across data of any type or source to gain deeper insights and drive impactful outcomes.

- Data Sharing
- Diverse Data
- Hybrid Cloud
- Massive Volumes
- Rapid Prototyping
- Real-Time Analytics
- Security & Compliance

Data Management
Ohio's self-service data management suite provides rich and secure capabilities to harness the power of the analytics platform leveraging User friendly and pre-configured technologies. Additionally, the suite 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
- Bring Your Own Tool (BYOT)
- Data Engineering
- Data Exploration
- Data Lineage
- Data Profiling
- Governance & Security
- Pre-Built Pipelines
- Self-Service Support

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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.2. Application Services

3.3.2.1. Enterprise Document Management Solution (DMS):

The Enterprise Document Management Solution (DMS) 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, e-mail and information archiving.

3.3.2.2. Electronic Data Interchange (EDI) Application Integration:

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 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.

3.3.2.3. Enterprise Business Intelligence (BI):

The State of Ohio Enterprise Business Intelligence (BI) service provides enterprise data warehousing, business and predictive analytics, and decision support solutions. By turning raw data into usable information, BI helps Users analyze policies and programs, evaluate operations, and drive decisions. The core information available for analysis includes:

Health and Human Services Information

- Ohio Benefits
- Medicaid Claims
- Medicaid Enrollment
- Medicaid Financial
- Medicaid Provider
- Long Term Care
- Medicare Claims

- Pharmacy

Financial Information

- General Ledger
- Travel and Expense
- Procure to Pay
- Capital Improvements
- Accounts Receivable
- Asset Management
- Budget/Planning
- Value Management
- Statewide Cost Allocation Plan
- Minority Business Enterprise (MBE) Program/Encouraging Diversity, Growth and Equity (EDGE) Program

Workforce and Human Resources

- Workforce Profile
- Compensation
- State of Ohio Payroll Projection Systems
- ePerformance
- Enterprise Learning Management

3.3.2.4. Enterprise eLicense:

Enterprise eLicense 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. 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

3.3.2.5. ePayment Business Solution:

The CBOSS ePayment Gateway 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 CBOSS ePayment Gateway 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 Telecheck services.

The CBOSS ePayment Gateway 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 SSAE16 SOC1 Type II.

3.3.2.6. 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.

3.3.2.7. 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 workflow-based application which provides flexibility and ease-of-use. ServiceNow 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 for the management of related fields, approvals, escalations, notifications and reporting needs.

Standard ServiceNowFeatures Include:

- **Incident Management** - Manage service disruptions and restore normal operation quickly.
- **Problem Management** - Identify the underlying cause of recurring incidents.
- **Change Management** - Minimize the impact of service maintenance.
- **Configuration Management** - Define and maintain a configuration management database (CMDB) for IT infrastructure.
- **Asset Management** - Manage assets and inventory records.
- **Service Catalog Management** – Automated process for goods and service requests.
- **Knowledge Management** - Gather, store and share knowledge within the organization.
- **Reporting** – Custom reporting.
- **Integration to AD, Event Monitoring, Discovery Tools, Exchange** – Integration to AD, Event Monitoring, Discovery Tools, Exchange – Integration with third-party applications.

- **Customized Portal Pages** – User friendly interface to create engaging and robust portals, dashboards, and applications.
- **Software Asset Management** – End to end software life cycle management on a single platform, to optimize spend and reduce compliance risk.
- **IT Operations Management (ITOM)** - Includes event management, service mapping, discovery, orchestration and cloud management.

3.3.2.8. 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:

1. **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability.
2. **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.
3. **Analytics and Business Intelligence** – Integration and delivery of analytics in the form of alerts, notifications and reports.
4. **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.

3.3.2.9. 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. Ohio businesses can use OBG to access various services and electronically submit transactions and payments. The OBG also offers the ability for business to view historical filings (and payments) and allows for business activities to be provided by a third-party provider of professional accounting services. 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 so that they may continue to manage the overall account relationship.

3.3.2.10. 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, 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
- Targeted Business Intelligence
- Tableau Analytics and Visualization

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting

Financial Management (FIN)

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

Human Capital Management (HCM)

- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration

3.3.2.11. Enterprise Geocoding Services (EGS):

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for online applications or large numbers of addresses can be processed in batch mode.

3.3.2.12. Geographic Information Systems (GIS) Hosting:

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Users can integrate enterprise-level GIS with map capabilities and spatial content into new or existing websites and applications.

Please explain how the State's 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.3. Data Center Services

3.3.3.1. Advanced Interactive eXecutive (AIX):

AIX is a proprietary version of the UNIX operating system developed by IBM. 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.

3.3.3.2. Backup:

The Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of 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. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

3.3.3.3. Data Center Co-Location:

The DAS OIT Co-Location service offers 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 24x7x365 and is accessible via electronic card key only.

3.3.3.4. Data Storage:

The services covered under 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, externally-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, which is not on a 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.

3.3.3.5. Distributed Systems DRaaS:

Distributed Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus. The service provides a private Disaster Recovery as a Service solution connected to the State of Ohio Computer Center (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.

3.3.3.6. 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 available for 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 bi-annually at IBM’s hot site location, during which DAS OIT’s mainframe computer infrastructure is restored. Once the mainframe system is operational, production applications are restored and extensive tests are conducted 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.

3.3.3.7. Mainframe Systems:

DAS OIT’s Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5,700 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. 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.

3.3.3.8. Metro Site Facility:

The Metro Site Facility Service provides a secondary, near real-time (measured in ms) 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 for the support of Virtual Server and Data Storage, providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area.

3.3.3.9. 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 providing solutions around availability, security and automation.
Server Virtualization includes:

- **DAS 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.

Please explain how the State's Data Center 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.4. Hosted Services

3.3.4.1. Database as a Service:

Database as a Service provides an enterprise database solution that is easy to use and simple to update without incurring the cost of setting up and maintaining an enterprise database environment through which scaling, load balancing, failover and backup can all be managed. DAS OIT Database Specialists ensure that all aspects of handling data are taken care of which includes, but is not limited to, storage, backups, tuning and security.

Current Database Solutions being offered:

- SQL Server
- Oracle
- DB2

Oracle Exadata DBaaS:

- **Starter/Small Database:** 2 Cores, 6GB Ram, 200GB min Storage, *Up to 2 databases
  Entry level database environment for small applications.
- **Medium Database:** 4 Cores, 8 GB Ram, 500GB Min Storage, *Up to 4 databases
  Medium sized database environment for DB consolidation.
- **Large Database:** 6 Cores, 12GB Ram, 1TB Min Storage, *Up to 6 Databases

Optimal service for large, complex database and data warehouse environments.

*The maximum number of databases is dependent upon the database size and actual usage.

Based on the model the proposed service model for DAS OIT includes the following structure:

- **Small**: 2 Core = 1 billable unit per month.
- **Medium**: 4 Cores = 2 billable units per month.
- **Large**: 6 Cores = 3 billable units per month.

3.3.4.2. Database Support:

Database Support provides technical assistance for database implementation and usage. Services utilized 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.5. IT Security Services

3.3.5.1. Secure Sockets Layer (SSL) Digital Certificate Provisioning:

SSL Digital Certificate Provisioning service provides SSL 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 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.6. IT Support Services

3.3.6.1. Enterprise End User Support:

Enterprise End User Support is a standardized, fully managed endpoint computing service. This Service uses enterprise tools and standards. This comprehensive service includes e-mail, network connectivity, device procurement, printer support, security policy maintenance, system monitoring, software updates and patching, software deployment to individuals and devices and inventory software and hardware. IT assets provided with the Enterprise End User Support include:

- Dedicated on-site technician
- Break/Fix
- Enterprise Image
- System Center Configuration Management (SCCM)
- Patch Management through SCCM
- Application packaging and deployment
- Asset management (hardware)
- Asset management (software)
- Application usage report provided upon request

3.3.6.2. Enterprise Virtual Desktop:

Enterprise Virtual Desktop service takes advantage of the Enterprise Private Cloud to store all electronic data via a virtual desktop. The service provides a platform with access to Microsoft Windows and State of Ohio business applications from any device, from any location, at any time.
The Enterprise Virtual Desktop service offers the following:

- **Hosted** - The unmanaged service provides an isolated and dedicated environment that is managed by DAS OIT. This hosted service includes a provisioning portal, a basic window image and a basic group policy for desktops but does not include management or deployment of specific software or desktop provisioning.
- **Managed** - The managed service provides an isolated and dedicated environment that is managed by DAS OIT including desktops and software deployment. The Managed service also includes all Hosted services, software packaging and updating, management of the operating system, deployments and updates.

Please explain how the State's IT Support 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.7. Messaging Services

3.3.7.1. Microsoft License Administration (Office 365):

The Office 365 service provides the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing access to 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, Skype for Business and OneNote), SharePoint, and OneDrive for Business. Microsoft Office Suite includes:

- Email in the Microsoft Cloud
- Office 365 ProPlus
- Skype for Business

- 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.8. Network Services

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

3.3.8.1. 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 regardless of location or device and deliver a consistent, reliable network access method.

3.3.8.2. Secure Authentication:

The DAS OIT Secure Authentication service provides a managed two-factor User authentication solution. 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 an environment.

3.3.8.3. Wireless as a Service:

Wireless as a Service is the IT Enterprise Wireless hosted network. 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 noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.9. Telephony Services

3.3.9.1. 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:

3.3.9.2. Toll-Free Services:

A service provided to incur telephone charges for incoming calls to an 8xx number.

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

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.

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.

3.3.9.4. Call Recording Services:

Call Recording Services for new VoIP profiles or modifying existing profiles.

3.3.9.5. Conferencing

This service offers a conferencing service via telephone lines. It provides voice conferencing capabilities within the network and participants can also join in from outside the network.

3.3.9.6. Fax2Mail:

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. Fax2Mail is completely “cloud-based” (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. 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.

3.3.9.7. Session Initiation Protocol (SIP) Call Paths:

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.

3.3.9.8. Site Survivability:

Provides reliable communications via multi-feature redundancy for centralized call processing.

3.3.9.9. 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 Voice/VoIP 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 noted 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 3.3.2 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.

Supplement S

State Information Security and Privacy Requirements

State Data Handling Requirements

Revision History:

Date:	Description of Change:	Version
10/01/2019	Updated the State Information Security and Privacy Requirements as well as the State Data Handling Requirements to align with current practices.	1.0

Table of Contents

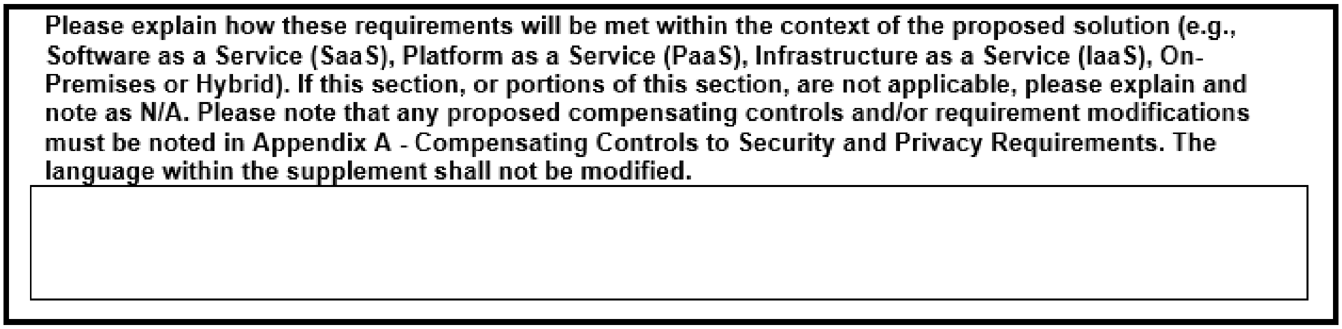
Page

Ohio Department of Administrative Services
Office of Information Security and Privacy
Main Number: 614-644-9391
30 E Broad Street, 19th Floor
Columbus, Ohio 43215
infosec.ohio.gov

State Information Security, Privacy and Data Handling Requirements Instructions

When providing a response to this Supplement, please follow the instructions below and frame your response as it relates to your proposed solution e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid.

1. After each specific requirement the offeror must provide a response on how the requirement will be met or indicate if it is not applicable and why.



Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

2. In the event there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it in Appendix A – Compensating Controls to Security and Privacy Requirements. Please be sure to provide a rationale for the change.

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: **Supplement 2 - Page 11**	**Example**: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **monthly**.	**Example:** Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **weekly**.	Per company policy vulnerability report are only provided to customers on a quarterly basis.

3. Upon completion, please submit the security supplement responses with the proposal documentation.

Overview and Scope

This supplement shall apply to the Contracts for all work, services, 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 conjunction with the delivery of work to the State and any access to State resources in conjunction with the delivery of work.

The selected Contractor will accept the security and privacy requirements outlined in this supplement in their entirety as they apply to the services being provided to the State. The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT security policies and standards.

This scope shall specifically apply 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.

- Any Contractor personnel or sub-contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

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 this contract shall prevail.

Please note that any proposed compensating controls to the security and privacy requirements outlined in this supplement are required to be identified in Appendix A – Compensating Controls to Security and Privacy Requirements. Contractors are asked not to make any changes to the language contained within this supplement.

State Requirements Applying to All Solutions

This section describes the responsibilities for both the selected Contractor and the State of Ohio as it pertains to State information security and privacy standards and requirements for all proposed solutions whether cloud, on-premises, or hybrid based. The Contractor will comply with State of Ohio IT security and privacy policies and standards as they apply to the services being provided to the State. A list of IT policy and standard links is provided in the State IT Policy and Standard Requirements and State IT Service Requirements supplement.

1. State Information Security and Privacy Standards and Requirements

The Contractor is responsible for maintaining the security of information in accordance with State security policies and standards. 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. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in statements of work and adhere to State policies and use procedures in a manner that does not diminish established State capabilities and standards.

1.1. The Offeror's Responsibilities

The offeror's responsibilities with respect to security services include the following, where applicable:

1.1.1. Support State IT security policies and standards, which includes the development, maintenance, updates, and implementation of security procedures with the State's review and approval, including physical access strategies and standards, User ID approval procedures, and a security incident action plan.

1.1.2. Support the implementation and compliance monitoring as per State IT security policies and standards.

1.1.3. If the Contractor identifies a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor shall identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

1.1.4. Support intrusion detection and prevention, including prompt State notification of such events and reporting, monitoring, and assessing security events.

1.1.5. Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. At a minimum, the Contractor shall provide vulnerability scan results to the State monthly.

1.1.6. Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a security incident response plan.

1.1.7. Manage and administer access to the systems, networks, system software, systems files, State data, and end users if applicable.

1.1.8. Install and maintain current versions of system software security, assign and reset passwords per established procedures, provide the State access to create User IDs, suspend and delete inactive User IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.

1.1.9. Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.

1.1.10. Perform physical security functions (e.g., identification badge controls and alarm responses) at the facilities under the Contractor's control.

1.2 The State's Responsibilities

The State will:

1.2.1. Develop, maintain, and update the State IT security policies, including applicable State information risk policies, standards, and procedures.

1.2.2. Provide the Contractor with contact information for security and program personnel for incident reporting purposes.

1.2.3. Provide a State resource to serve as a single point of contact, with responsibility for account security audits.

1.2.4. Support intrusion detection, prevention, and vulnerability scanning pursuant to State IT security policies.

1.2.5. Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.

1.2.6. Provide audit findings material for the services based upon the security policies, standards and practices in effect as of the effective date and any subsequent updates.

1.2.7. Assist the Contractor in performing a baseline inventory of User IDs for the systems for which the Contractor has security responsibility.

1.2.8. Authorize user IDs and passwords for State personnel for the system's software, software tools and network infrastructure systems and devices under Contractor management.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

1.3. Periodic Security and Privacy Audits

The State will be responsible for conducting periodic security and privacy audits and will generally utilize members of the Office of Information Security and Privacy, the Office of Budget and Management – Office of Internal Audit, and the Auditor of State, depending on the focus area of the audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

If a security or privacy issue exists in any of the IT resources furnished to the Contractor by the State (e.g., code, systems, computer hardware and software), the State will have responsibility to address or resolve the issue. The State may elect to work with the Contractor, under mutually agreeable terms for resolution services or the State may elect to address the issue independent of the Contractor. The Contractor is responsible for resolving any security or privacy issues that exist in any of the IT resources they provide to the State.

For in-scope environments and services, all new systems implemented or deployed by the Contractor must comply with State security and privacy policies and standards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.1. State Penetration and Controls Testing

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/privacy functions and procedures, data storage and encryption methods, backup/restoration processes, as well as security penetration testing and validation. The State may utilize a third-party Contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met.

State acceptance testing will not proceed until the Contractor cures, according to the State's written satisfaction, all findings, gaps, errors or omissions pertaining to the audit. Such testing will be scheduled with the Contractor at a mutually agreed upon time.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.2. System Security Plan

A completed System Security Plan must be provided by the Contractor to the State and the primary point of contact from the Office of Information Security and Privacy no later than the end of the project development phase of the System Development Life Cycle (SDLC). The plan must be updated annually or when major changes occur within the solution. The templates referenced below are the required format for submitting security plans to the State.

Ohio Security Plan
Template.docx

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.3. Risk Assessment

A Risk Assessment report completed within the past 12 months must be provided to the State and the primary point of contact from the Office of Information Security and Privacy no later than the project development phase of the System Development Life Cycle (SDLC). A new risk assessment must be conducted every two years, or as a result of significant changes to infrastructure, a system or application environment, or following a significant security incident.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.4. Security and Data Protection

All solutions must classify data per State of Ohio IT-13 Data Classification policy and per the sensitivity and criticality, must operate at the appropriate baseline (low, moderate, high) as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations” (current, published version), be consistent with Federal Information Security Management Act (“FISMA 2014”) requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. The solution must provide the State’s systems administrators with 24x7 visibility into the services through a real-time web-based “dashboard” capability that enables them to monitor, in real or near real time, the services’ performance against the established service level agreements and promised operational parameters.

If the solution is cloud based, the Contractor must obtain an annual audit that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (“SSAE”) No. 16, 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 Agreement. The audit will be at the sole expense of the Contractor and the results must be provided to the State within 30 days of its completion each year.

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.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.5. Data

1.5.1. “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.

1.5.2. “Sensitive Data” is any type of data that presents a high or moderate degree of risk if released or disclosed without authorization. Sensitive Data includes but not limited to:

1.5.2.1. Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.

1.5.2.2. Federal Tax Information (FTI) under IRS Special Publication 1075,

1.5.2.3. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA)

1.5.2.4. Criminal Justice Information (CJI) under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy.

1.5.2.5. 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.

1.6. Protection and Handling the State’s Data

To protect State Data as described in this contract, 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:

1.6.1. Maintain in confidence State Data it may obtain, maintain, process, or otherwise receive from or through the State in the course of the contract.

1.6.2. Use and permit its employees, officers, agents, and subcontractors to use any State Data received from the State solely for those purposes expressly contemplated by the contract.

1.6.3. 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 this contract or required by applicable law, regulation, or court order.

1.6.4. 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.

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

1.6.6. Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data.

1.6.7. Align with existing State Data security policies, standards and procedures designed to ensure the following:

1.6.7.1. Security and confidentiality of State Data

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

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

1.6.8. Suggest and develop modifications to existing data security policies and procedures or draft new data security policies and procedures when gaps are identified.

1.6.9. Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.

1.6.10. Give access to State Data only to those individual employees, officers, agents, and sub-contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this contract.

1.6.11. Maintain appropriate identification and authentication processes for information systems and services associated with State Data.

1.6.12. Any Sensitive Data at rest, transmitted over a network, or taken off-site via portable/removable media must be encrypted pursuant to the State's data encryption standard, Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," and Ohio Administrative Policy IT-14, "Data Encryption and Securing State Data."

1.6.13. Any data encryption requirement identified in this supplement means encryption that complies with National Institute of Standards and Technology's Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number.

1.6.14. Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.

1.6.15. Implement and manage security audit logging on information systems, including computers and network devices.

1.6.16. Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State. The State will be responsible for all costs incurred by the Contractor for compliance with this provision of this subsection.

1.6.17 Upon request by the State, promptly destroy or return to the State, in a format designated by the State, all State Data received from or through the State.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.7. Contractor Access to State Network Systems and Data

The Contractor must maintain a robust boundary security capability that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these ports, and disabling all others.

To do this, the Contractor must:

1.7.1 Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.

1.7.2. Use multifactor authentication to limit access to systems that contain Sensitive Data, such as Personally Identifiable Information.

1.7.3. Assume all State Data is both confidential and critical for State operations. The Contractor's security policies, plans, and procedures for the handling, storage, backup, access, and, if appropriate, destruction of State Data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.

1.7.4. Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Contractor's infrastructure associated with the State Data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State Data.

1.7.5. Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State data is stored. The method of securing the State Data must be in alignment with the required data classification and risk assessment outcomes, and may include secure overwriting, destruction, or encryption of the State data before transfer of control in alignment with NIST SP 800-88. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this contract.

1.7.6. Have a business continuity plan in place that the Contractor tests and updates no less than annually. The plan must address procedures for responses to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains State Data in case of loss of State Data at the primary site. The Contractor's backup solution must include plans to recover from an intentional deletion attempt by a remote attacker exploiting compromised administrator credentials.

The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the Sensitive Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

1.7.7. Not allow State Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this contract. If necessary, for such performance, the Contractor may permit State Data to be loaded onto portable computing devices or portable storage components or media only if adequate security measures are in place to ensure the integrity and security of State Data. Those measures must include a policy on physical security and appropriate encryption for such devices to minimize the risk of theft and unauthorized access as well as a prohibition against viewing sensitive or confidential data in public or common areas.

1.7.8. Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted across any data network.

1.7.9. Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.8. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including transport layer security (TLS) and public key authentication, signing and/or encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided public key infrastructure (PKI). Multifactor authentication must be employed for users with privileged network access by State provided solutions.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.9. Portable Devices and Media

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such devices to the State in writing as defined in Section 3 Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues. The Contractor must have a written policy that defines procedures for how the Contractor must detect, evaluate, and respond to adverse events that may indicate an incident or an attempt to attack or access State Data or the infrastructure associated with State Data.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2. State and Federal Data Privacy Requirements

All systems and services must be designed and must function according to Fair Information Practice Principles (FIPPS), which are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability, and auditing.

To the extent that personally identifiable information (PII) in a system is “protected health information” under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the FIPPS principles must be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in a system that is not “protected health information” under HIPAA, the FIPPS principles must still be implemented and, when applicable, aligned to other laws or regulations.

2.1 Contractor Requirements

The Contractor specifically agrees to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to the work associated with this Contract including but not limited to:

2.1.1. United States Code 42 USC 1320d through 1320d-8 (HIPAA).

2.1.2. Code of Federal Regulations for Public Health and Public Welfare: 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR164.502 (e) and 164.504 (e).

2.1.3. Ohio Revised Code (ORC) 1347.01, 1347.04 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5160.39, 5168.13, and 5165.88.

2.1.4. Corresponding Ohio Administrative Code Rules and Updates.

2.1.5. Systems and services must support and comply with the State’s security operational support model, which is aligned to NIST SP 800-53 (current, published version).

2.1.6. IRS Publication 1075, Tax Information Security Guidelines for federal, state, and local agencies.

2.1.7. Criminal Justice Information Systems Policy.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.2. Federal Tax Information (FTI)

All computer systems receiving, processing, storing, or transmitting Federal Tax Information (FTI) must meet the requirements defined in IRS Publication 1075.

2.2.1. IRS 1075 Performance Requirements:

In the performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

2.2.1.1. All work involving FTI will be done under the supervision of the Contractor or the Contractor's employees.

2.2.1.2. The contractor and the contractor’s employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

2.2.1.3. Any federal tax return or return information made available in any format shall be used only for the purposes of performing this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the Contractor is prohibited.

2.2.1.4. All federal tax returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

2.2.1.5. The Contractor certifies that the IRS data processed during the performance of this contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the Contractor after the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.

2.2.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the State or its designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the State or its designee with a Statement containing the date of destruction, description of material destroyed, and the method used.

2.2.1.7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in the IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical IRS 1075 controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

2.2.1.8 No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

2.2.1.9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

The agency will have the right to void the Contract if Contractor fails to provide the safeguards described above.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.2.2. IRS 1075 Criminal/Civil Sanctions

2.2.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2.2.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

2.2.2.3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2.2.3. Inspection

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor for inspection of the facilities and operations performing any work under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual, and/or automated scanning tools to perform compliance and vulnerability assessment of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with contract safeguards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.3. Disclosure

Disclosure to Third Parties. This Contract must not be deemed to prohibit disclosures in the following cases:

2.3.1. Required by applicable law, regulation, court order or subpoena; provided that, 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, Contractor must notify the State within 24 hours in order that the State may have the opportunity to seek a protective order or take other appropriate action. 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, Contractor is compelled as a matter of law to disclose the information provided by the State, 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, 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 Contractor must use commercially reasonable efforts to obtain confidential treatment for the information:

2.3.1.1. To State auditors or regulators.

2.3.1.2. 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.

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

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.4. Background Investigations of Contractor Personnel

Contractor agrees that (1) the State of Ohio will conduct background investigations on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no ineligible personnel will perform Sensitive Services under this contract. The term “ineligible personnel” means 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.

“Sensitive Services” means those services that (i) require access to customer, consumer, or State employee information, (ii) relate to the State’s computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities.

Contractors who will have access to Federal Tax Information (FTI) or Criminal Justice Information (CJI) must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information. In addition, existing Contractors with access to FTI or CJI that have not completed a background investigation within the last 5 years must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information.

FTI or criminal justice background investigations will include:

2.4.1. FBI Fingerprinting (FD-258)

2.4.2. Local law enforcement agencies where the employee has lived, worked and/or attended school within the last five years

2.4.3. Citizenship/residency eligibility to legally work in the United States

2.4.4. New employees must complete USCIS Form I-9, which must be processed through the Federal E-Verify system

2.4.5. FTI training, with a 45 day wait period

In the event that the Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3. Contractor Responsibilities Related to Reporting of Concerns, Issues, and Security/Privacy Issues

3.1. General

If, over the course of the Contract a security or privacy issue arises, whether detected by the State, a State auditor, or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any contracted service associated with this Contract, the Contractor must:

3.1.1. Notify the State of the issue or acknowledge receipt of the issue within two (2) hours.

3.1.2. Within forty-eight (48) hours from the initial detection or communication of the issue from the State, present a potential exposure or issue assessment document to the State account representative and the State Chief Information Security Officer with a high-level assessment as to resolution actions and a plan.

3.1.3. Within four (4) calendar days, and upon direction from the State, implement, to the extent commercially reasonable, measures to minimize the State's exposure to the security or privacy issue until such time as the issue is resolved.

3.1.4. Upon approval from the State, implement a permanent repair to the identified issue at the Contractor's cost.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any Sensitive Data by the Contractor or any of its Subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its Subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

3.2.1. Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized disclosure or intrusion.

3.2.2. Investigate and determine if an intrusion and/or disclosure has occurred.

3.2.3. Fully cooperate with the State in estimating the effect of the disclosure or intrusion and fully cooperate to mitigate the consequences of the disclosure or intrusion.

3.2.4. Specify corrective action to be taken.

3.2.5. Take corrective action to prevent further disclosure and/or intrusion.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

The following are the responsibility of the Contractor to provide at its own cost:

3.3.1. The Contractor must, as soon as is practical, make a report to the State including details of the disclosure and/or intrusion and the corrective action the Contractor has taken to prevent further disclosure and/or intrusion. The Contractor must, in the case of a disclosure, cooperate fully with the State to notify the affected persons as to the facts and circumstances of the disclosure of the Sensitive Data. Additionally, the Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies that have jurisdiction to investigate a disclosure and/or any known or suspected criminal activity.

3.3.2. If, over the course of delivering services to the State under this statement of work for in-scope environments, the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams, the Contractor must notify the State within two (2) hours. This notification must not minimize the more stringent service level contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach must take precedence over this notification. The State may elect to work with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

3.3.3. If the Contractor identifies 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.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.4. Security Incident Reporting and Indemnification Requirements

3.4.1. The Contractor must report any security incident of which it becomes aware. For the purposes of this document, “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It does not mean unsuccessful log-on attempts, denial of service attacks, unsuccessful network attacks such as pings, probes of firewalls, port scans, or any combination of those, as long as there is no unauthorized access, acquisition, use, or disclosure of Sensitive Data as a result.

3.4.2. In the case of an actual security incident that may have compromised Sensitive Data, the Contractor must notify the State in writing within two (2) hours of the Contractor becoming aware of the breach. The Contractor is required to provide the best available information from the investigation.

3.4.3. In the case of a suspected incident, the Contractor must notify the State in writing within twenty-four (24) hours of the Contractor becoming aware of the suspected incident. The Contractor is required to provide the best available information from the investigation.

3.4.4. The Contractor must fully cooperate with the State to mitigate the consequences of an incident/suspected incident at the Contractor’s own Cost. This includes any use or disclosure of the Sensitive Data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this contract by an employee, agent, or Subcontractor of the Contractor.

3.4.5. The Contractor must give the State full access to the details of the breach/suspected breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate at the Contractor’s own cost.

3.4.6. The Contractor must document and provide incident reports for all such incidents/suspected incidents to the State. The Contractor must provide updates to incident reports until the investigation is complete at the Contractor’s own cost. At a minimum, the incident/suspected incident reports will include:

3.4.6.1. Data elements involved, the extent of the Data involved in the incident, and the identification of affected individuals, if applicable.

3.4.6.2. 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 incident.

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

3.4.6.4. A description of the probable causes of the incident.

3.4.6.5. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval.

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

3.4.7. In addition to any other liability under this contract related to the Contractor’s improper disclosure of State Data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year’s identity theft protection service on behalf of any individual or entity whose Sensitive Data is compromised while it is in the Contractor's possession. This service will be provided at Contractor's own cost. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individual's credit history through those services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

4.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this includes:

4.1.1. Deviations from the hardware baseline.

4.1.2. Inventory of information types by hardware device.

4.1.3. Software inventory compared against licenses (State purchased).

4.1.4. Software versions and then scans of versions against patches distributed and applied.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.2. Security Standards by Device and Access Type

The Contractor must:

4.2.1. Document security standards by device type and execute regular scans against these standards to produce exception reports.

4.2.2. Document and implement a process for any required remediation.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.3. Boundary Defenses

The Contractor must:

4.3.1. Work with the State to support the denial of communications to/from known malicious IP addresses.

4.3.2. Ensure that the system network architecture separates internal systems from DMZ and extranet systems.

4.3.3. Require the use of two-factor authentication for remote login.

4.3.4. Support the State's monitoring and management of devices remotely logging into the internal network.

4.3.5. Support the State in the configuration of firewall session tracking mechanisms for addresses that access the solution.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.4. Audit Log Reviews

The Contractor must:

4.4.1. Work with the State to review and validate audit log settings for hardware and software.

4.4.2. Ensure that all systems and environments have adequate space to store logs.

4.4.3. Work with the State to devise and implement profiles of common events from given systems to reduce false positives and rapidly identify active access.

4.4.4. Provide requirements to the State to configure operating systems to log access control events.

4.4.5. Design and execute bi-weekly reports to identify anomalies in system logs.

4.4.6. Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.5. Application Software Security

The Contractor must:

4.5.1. Perform configuration review of operating system, application, and database settings.

4.5.2. Ensure software development personnel receive training in writing secure code.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A – Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.6. System Administrator Access

The Contractor must:

4.6.1. Inventory all administrative passwords (application, database, and operating system level).

4.6.2. Implement policies to change default passwords in accordance with State policies, following any transfer or termination of personnel (State, existing Materials and Supplies Vendor, or Contractor).

4.6.3. Configure administrative accounts to require regular password changes.

4.6.4. Ensure user and service level accounts have cryptographically strong passwords.

4.6.5. Store passwords in a hashed or encrypted format.

4.6.6. Ensure administrative accounts are used only for administrative activities.

4.6.7. Implement focused auditing of administrative privileged functions.

4.6.8. Configure systems to log entry and alert when administrative accounts are modified.

4.6.9. Segregate administrator accounts based on defined roles.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.7. Account Access Privileges

The Contractor must, in alignment with policy requirements:

4.7.1. Review and disable accounts not associated with a business process.

4.7.2. Create a daily report that includes locked out accounts, disabled accounts, etc.

4.7.3. Implement a process for revoking system access.

4.7.4. Automatically log off users after a standard period of inactivity.

4.7.5. Monitor account usage to determine dormant accounts.

4.7.6. Monitor access attempts to deactivated accounts through audit logging.

4.7.7. Profile typical account usage and implement or maintain profiles to ensure that security profiles are implemented correctly and consistently.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.8. Additional Controls and Responsibilities

The Contractor must meet with the State no less frequently than annually to:

4.8.1. Review, update and conduct security training for personnel, based on roles.

4.8.2. Review the adequacy of physical and environmental controls.

4.8.3. Verify the encryption of Sensitive Data in transit.

4.8.4. Review access controls based on established roles and access profiles.

4.8.5. Update and review system administration documentation.

4.8.6. Update and review system maintenance policies.

4.8.7. Update and review system and integrity policies.

4.8.9. Review and implement updates to the System security plan.

4.8.10 Update risk assessment policies and procedures.

4.8.11 Update and implement incident response procedures.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

Appendix A – Compensating Controls to Security and Privacy Supplement

In the event that there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it below and provide a proposed language change as well as a rationale for the change.

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: **Supplement 2 - Page 11**	**Example**: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **monthly.**	**Example:** Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **weekly**.	Per company policy vulnerability report are only provided to customers on a quarterly basis.

JFS-DAS Security Supplement Addendum

In accordance with the Governor DeWine’s executive order 2019-15D:

https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders/2019-15d

ODJFS is required to participate in the InnovateOhio Platform.

IOP - Identity & Access Management

The InnovateOhio Platform (IOP) provides a secure digital identity experience including an intuitive and interactive user experience for Ohio’s citizens, businesses, and employees. The program provides centralized administration and synchronization of user identities to enable user provisioning and de-provisioning of identity and access for state systems. The *Application or Service* must, for all State/County employees, Businesses (Providers), and Citizens, provide single sign-on capabilities through integration with the State's Enterprise Identity Management system called Innovate Ohio Platform (IOP) leveraging IBM’s Identity Federation.

IOP is aligned around four distinct pillars that support a consistent user experience for State of Ohio services constituents:

Enterprise Identity Pillar: Enterprise ID Management Framework having the following capabilities:

- User Provisioning
- Single Sign-on
- Identity Proofing
- 2-Factor Authentication (2FA)
- Federation
- Logging and Monitoring

Fraud and Risk Analytics Pillar: A comprehensive, risk-focused fraud detection and analytics service that can detect, prevent, analyze, and report on fraudulent activities in real time.

This enterprise, thin-layer tool is built upon the Federal Data Science Framework and provides:

- Continuous Machine Learning
- Scalable and Accessible Big Data
- Real-time Detection
- Key Graphics

User Experience Pillar: The User Experience Pillar supports an enhanced user and agency experience through consistent look and feel, optimized flows and functionalities and reduced redundancy.

- **User Interface:** (To the extent possible) standardized look and feel, navigation, and presentation of web sites, portals, and applications using a standard digital interface.
- **User Experience:** User-centric design, processes, tasks, and functions that support quicker, easier, and more secure access to and interaction with state agencies.
- **Agency Experience:** State-wide, centralized access point that adheres to the desired user experience and user interface, supported by standard tools, methods, and digital tool kits.

Platform and Portal Services Pillar: Provide an experience that promotes privacy, choice, and flexibility for citizens, businesses, and employees by:

- Enabling better, more secure access to an ever-growing set of digital services and self-help features across the state through a single proofed identity
- Enabling the state as an organization to consolidate historical transactions and cross-program / agency data to lead a better user experience

Required Interfaces with IOP:

For all Applications and Services that require authentication and/or authorizations:

Federated Single Sign-on: Application must support federated single sign-on using SAML 2.0 OR using Open ID Connect (OIDC) for identity assertion to authenticate the user to the Application

Authorization-Based Assertion Attributes: Application, optionally but preferred, would support Token assertions to determine appropriate authorizations (roles/permissions) for the individual, upon sign-in, based upon supplied Group membership attribute(s) (or other attributes as needed).

Automation of Provisioning / de-provisioning: Application, optionally but preferred, must support either:

1. A connector that is available within the IBM Identity suite, out of the box, to automate Agency user provisioning and de-provisioning tasks.
2. The Application has SOAP or REST Service(s) available that the IBM Identity suite (ISIM) can call to automatically perform provisioning and de-provisioning tasks.

Provisioning Tasks available:

- Create, or associate, an identity in the application for authentication and single sign-on (e.g. Just in Time provisioning or achieved through Group to role inspection above).
- Assign and Change an identity's assignment to specific Roles/Permissions within the application for authorization (or achieved through Group to role inspection above).

De-provisioning Tasks available:

- Delete, or un-associate, an identity in the application to revoke the person's ability to authenticate (or achieved through Group to role inspection above).
- Remove or alter specific Roles/Permissions per identity within the application to remove authorization (or achieved through Group to role inspection above).

Device Authentication: Tracking device information (IP Address, OS, etc.) is required by the application. Application, optionally but preferred, would support device authentication in conjuncture with the IOP Framework above. This will support the ability to prompt for additional security validation /authentication to user in the event the device is not recognized. Such as prompting for two-factor authentication, or having the user submit to ID Proofing, or challenge response questions for additional identity validation. Once the device is identified and tied to User identity, these questions can optionally not be presented or can periodically be reaffirmed based on business requirements.

IOP – Data Analytics

All Applications must make data available to the InnovateOhio Platform for secure, resilient Data Storage, reporting, analytics and data sharing across all Cabinet Agencies, Boards, and Commissions.

In summary, ODJFS is to: (1) Make data available to the InnovateOhio Platform for storage (staging before sharing) upon request of InnovateOhio; and (2) Share data pursuant to ORC 125.32 and at the direction of InnovateOhio, acknowledging any Federal restrictions or privacy requirements.

A standing Data Sharing Protocol outlines procedures and responsibilities of DAS and agencies for use of the InnovateOhio Platform under authority of ORC 125.32 and Executive Order 2019-15D.

DAS manages the InnovateOhio Platform which consists of a set of advanced data and analytics computing technologies including a robust data governance, security and privacy protection foundation to enable usage of state data and to protect data maintained on the platform. Note that a distinction must be made between 1) an agency providing and hosting data on the platform and 2) an agency approving the use of data for analysis. When an agency provides and hosts data on the InnovateOhio Platform, the agency is not granting "use" of the data to any party including DAS. DAS's responsibility is to manage the platform as described within this protocol under and pursuant to ORC 125.18 and ORC 125.32. DAS is not given permission to "use" agency data unless the owning agency specifically approves.

ORC 125.32 states that, "A state agency that provides data under the program retains ownership over the data. Notwithstanding any other provision of the Revised Code, only the state agency that provides data under the program may be required under the law of this state to respond to requests for records or information regarding the provided data, including public records requests, subpoenas, warrants, and investigatory requests."

Encryption

Personally identifiable information (PII), or confidential personal information (CPI - as defined in Ohio Revised Code 1347), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. One of the key security controls to protecting PII/CPI is Encryption. Encryption is to be utilized for PII/CPI data on all three states of existence:

Data at Rest: Data at Rest refers to inactive data which is stored physically in any digital form. This refers to both Structured (databases) and unstructured Data (files).

PII/CPI Data at Rest must be protected in one of the following methods:

- Encrypt the Entire Database with Transparent Data Encryption (TDE)
- Table/ Column or Field Level Encryption can be used within the Database Tables to encrypt just the PII/CPI

Ensure that any temporary representations (temp files or folders/ exports/ backups / reports, etc.) of PII/CPI is encrypted in that current state.

  - Applying newer encryption technologies and techniques, such as “homomorphic encryption” can be used to meet this requirement.

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms.

Data in Motion: Data in Motion refers to data which is being transferred across some network or transmission media.

PII/CPI Data in Motion must be protected in one of the following methods:

- Encrypt the Entire transmission using HTTPS or IPSEC (or equivalent protocols) between all devices and tiers (such as UI > APP > DB Tiers)
- Encrypt the PII/CPI data only in transmission (Example: SOAP message using WS-Security)

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms / Modules. When using the Transport Layer Security (TLS), TLS version 1.2 or higher must be used.

Data in Use: Data in Use refers to data actively being used across the network or temporarily residing in memory, or any data not currently “inactive”.

PII/CPI Data in Use must be protected in the following methods:

- Implement Memory protections, at a minimum, of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) within Hardware and/or Software.
- Sessions must be unique to each authenticated user and be protected in way that meets the Open Web Application Security Project (OWASP)’s Application Security Verification Standard (ASVS).
- Application will use per user or session indirect object references where possible. All direct object References, from an untrusted source, must include an access control check to ensure the user is authorized for the requested object.
- Ensure that authentication /authorization checks are performed at each object at the controller and business logic levels, and not just at the presentation layer.
- Prevent Injection attacks by using a parameterized API or escape special characters using the specific escape syntax for that interpreter. Also, in addition, positive or “white list” input validation must be used.
- Device configurations must confirm to industry best practices for hardening (CIS Benchmarks).
- Components, such as libraries, frameworks, or other software modules used in development must be identified and a list provided to ODJFS at the conclusion of the project. A supported version of these components must be used at time of the contract.
- Autocomplete must be disabled on forms collecting PII/CPI, and caching must be disabled for pages that contain PII/CPI.
- Avoid the use of redirects and forwards as much as possible. When used, any such destination parameters must be a mapped value, and that server-side code translates this mapping to the target URL.

Audit Logging

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. (Source NIST SP 800-92 "Guide to Computer Security Log Management")

ODJFS is required, for compliance to Federal and State Laws, codes, standards, and guidelines, to perform audit logging and management of those logs for its information systems.

Logging Requirements

The following Application Events must be record in the audit log(s) for the Information System.

Required Audit Events:

1. User account management activities (user creation, deletion, modification),
2. Application shutdown,
3. Application restart,
4. Application errors,
5. Failed and successful log-on(s),
6. Security policy modifications,
7. Use of administrator privileges,
8. All changes to logical access control authorities (e.g., rights, permissions, role assignment),
9. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services,
10. Access to Personally Identifiable Information (PII – Also known as Confidential Personal Information (CPI) by Ohio Law),
11. Modification to Personally Identifiable Information (PII) - Also known as Confidential Personal Information (CPI)by Ohio Law),
12. File creation, deletion, or modification by the application (PDF, CSV, etc. - if Applicable).

Minimum Logging Requirements for Each Event

The following are the minimum required details that must be captured with each recorded event:

1. Identity of any user/subjects associated with the event (Who – user/group/device/system),
2. Event Information (What happened),
3. What Time the event occurred (When),
4. Subsystem or application the event occurred in (Where),
5. And the success/failure of the event (if applicable).

Audit Record Generation Services

All Applications, in the event of audit log processing failure (the application is unable to write to the security log/ log service) shall:

1. Notify appropriate personnel of the audit log processing failure, and
2. shall either:
   a. Stop all processing of further request s until the audit log processing is restored, or
   b. Queue all audit events to disk, until such time as the audit log processing is restored or the storage allocation is filled.

If storage allocation is full, the application shall stop all processing of all further requests until the audit log processing is restored.

Audit Retention, Aggregation, and Analysis

Applications are required to send the Audit Event Log information, through standard processes (such as SYSLOG) or through add-ons, to the Agencies Enterprise Log Management (ELM) Tool – Splunk and Enterprise Security Information and Event Management (SIEM) – QRadar.

Any required third-party tools or services to achieve this requirement, the vendor must acquire, purchase, and setup.

Audit Log information must be sent security to ODJFS ELM and/or SIEM tools and CPI Log repository (when applicable), using encryption methods that use compliant NIST FIPS 140-2 Encryption Algorithms / Modules.

Development Security

Data Set used in Development

All Data sets used in non-production environments (Development, Quality Testing, User Acceptance testing, etc.) must be generated or masked data or data sets (not real production data). Except, where approved by Agency Security Official, and using the same set of security controls that are in place for the non-production environment as the production environment. Masked or generated data or data sets can be generated by ODJFS for these purposes.

DevOps Vulnerability Scanning

Applications being developed for hosting by the state (on-premise) must adhere to ODJFS DevOps pipeline AppSec tools and processes. This includes both Static (code or white-box scanning) and Dynamic (application or black-box scanning) vulnerability scanning. Additionally, any libraries or components used in the solution must be free of known critical or severe vulnerabilities and be scanned/evaluated by the ODJFS Software Composition Analysis (SCA) tool.

Hosted Solutions or Software as a Service (SaaS) Applications or Services. The vendor must provide proof that these scans are being performed and evaluated internally as part of their SDLC/DevOps processes, or by third Party compliance assessment certification/attestation (FedRAMP, ISO 27001, OWASP ASVS, CSA STAR, etc.).