REQUEST FOR PROPOSALS (RFP)

RFP Number: MHA17375

The Ohio Department of Mental Health and Addiction Services (MHAS), OIS, is requesting proposals for:

Windows Server Migration 2008
Lotus Notes

For the Period: **State Fiscal Year 2021 - July 1, 2021 through June 30, 2021**

RFP Issued: 3/29/2021
Inquiry Period Begins: 3/29/2021
Inquiry Period Ends: 4/10/2021
Proposals Due: 4/12/2021 @ 2:00 pm EST

Submit Proposals via e-mail to:

The Ohio Department of Mental Health and Addiction Services
OhioMHASBidOpportunity@mha.ohio.gov

This RFP consists of ninety one (91) pages. Please verify that you have a complete copy.

Please submit all inquiries about this RFP through the State Procurement web site at www.ohio.gov/procure. Please refer to Part Three of this RFP, "General Instructions", for instructions on submitting inquiries through the State Procurement web site. All responses to inquiries submitted by Proposers will be posted on the State Procurement website for viewing by all prospective Proposers.

Ohio | Department of Mental Health and Addiction Services

PART ONE: STRUCTURE OF THIS RFP

PARTS

Part One	Structure of this RFP
Part Two	Information on requested services
Part Three	General Instructions
Part Four	Evaluation of Proposals
Part Five	Contract Award

ATTACHMENTS

Appendix 1 – Standard Affirmation and Disclosure Form

- Standard Affirmation and Disclosure Form must be signed by an authorized official of Proposer's organization and must be included for any proposal to be scored

Appendix 2 – Contractor Information Form

- Contractor Information Form must be completed and submitted with the proposal.

PART TWO: SERVICES REQUESTED INFORMATION

I. MISSION & GUIDING PRINCIPLES

The mission of the Ohio Department of Mental Health and Addiction Services (MHAS) is to provide statewide leadership of a high-quality mental health and addiction prevention, treatment and recovery system that is effective and valued by all Ohioans. MHAS strives to be a national leader in implementing a comprehensive, accessible, and quality-focused system of addiction and mental health care and wellness for all Ohio citizens.

II. PURPOSE

The Ohio Department of Mental Health and Addiction Services (MHAS) is seeking proposals from qualified contractors to migrate a Lotus Notes Application running Windows Server 2008 onto a Window Server 2019 within 30 days after purchase order receipt date.

III. BACKGROUND

As part of Microsoft removing support from Windows Server 2008. The State of Ohio is executing a server migration from Windows Server 2008 to Windows Server 2019. This project reduces annual maintenance expense related to all applications supported by Windows 2008 Server.

As such MHAS currently has a Lotus Notes application installed in our Data Center running on Windows Server 2008 which requires remediation to Windows Server 2019.

IV. SCOPE OF WORK AND DELIVERABLES

The following scope of work is:
-
Install Lotus Notes Application onto a Windows 2019 Server
- Successful migrate database information onto a Window 2019 Server
- Ensure integration testing (IST) meets the success criterion
- Provide system configuration information to MHAS OIS System Engineering
- Provide a 30-day Application and Data Migration installation warranty
- Provide remote Go Live Support if required.

V. MINIMUM QUALIFICATIONS OF CONTRACTOR

Vendor must have extensive (more than 7-years) experience in system and data migrations

Vendor must have extensive (more than 7-years) experience migrating Lotus Notes Applications

Contractor shall not be subject to an “unresolved” finding for recovery under Section 9.24 of Ohio Revised Code.

VI. ETHICAL AND CONFLICT OF INTEREST REQUIREMENTS

No contractor or individual, company or organization seeking a contract shall promise or give to

any MHAS employee any item of value that is of such character as to manifest a substantial and improper influence upon the employee with respect to his or her duties.

No contractor or individual, company or organization seeking a contract shall solicit any MHAS employee to violate any of the conduct requirements for employees.
Any contractor acting on behalf of MHAS shall refrain from activities that could result in violations of ethics and/or conflicts of interest. Any contractor or potential contractor who violates the requirement and prohibitions defined Section 102.03 or Section 102.04 of the Ohio Revised Code is subject to termination of the contract or refusal by MHAS to enter into a contract.

PART THREE: GENERAL INSTRUCTIONS

The following sections provide a calendar of events, details on how to respond to this RFP and how to get more information about this RFP. All responses must be complete and in the prescribed format.

I. CALENDAR OF EVENTS & ONLINE INFORMATION

The schedule for this RFP is given below and is subject to change. MHAS may change this schedule at any time. If MHAS changes the schedule before the Proposal Due Date, it will do so through an announcement on the State Procurement web site area for this RFP at the following link: http://procure.ohio.gov/proc/index.asp. The web site announcement will be followed by an addendum to this RFP, which also will be made available through the same State Procurement web site.

It is each prospective Proposer's responsibility to check the State Procurement web site's question-and-answer area for this RFP for current information and the calendar of events scheduled through award of any contract.

Other than by adherence to the RFP Inquiry process, set forth below, no contact related to this RFP shall be made with MHAS until a contract award is announced. Notwithstanding this prohibition, MHAS, at its sole discretion, may request additional information as part of the review process outlined below.

Firm Dates

RFP Issued:	3/29/2021
Inquiry Period Begins:	3/29/2021
Inquiry Period Ends:	4/10/2021 8:00 am
Proposal Due Date:	4/12/2021 @ 2:00 pm EST

Estimated Dates

Contract Award Notification: 5/1/2021
Issuance of Purchase Order: To be determined

II. PROPOSAL FORMAT

Proposals must be prepared in accordance with instructions in this section. The proposal must clearly outline how each of the deliverables of Part 2 Section IV will be completed and with the time frames specified in that same section.

To be accepted, a proposal must include a technical proposal and a cost proposal as described in this section, contain all the information specified for each of the categories listed in this section, and meeting the requirements of this section

A. Technical Proposal

a. Transmittal letter includes:
- Identifies the bidder
- The name, title, address, and telephone number of the proposer's contract person with authority to answer questions concerning the RFP
- The name, title, address, telephone number, and email address of the

proposer's contact person with authority to execute a contract on behalf of the proposer.

b. Organizational experience including:
   - Information on the background of the firm or individual, including background information of any subcontractor(s)
   - Any prior experience relevant to this RFP (includes current contact names and phone numbers for these references), and a list of similar projects currently underway by the proposer or by any subcontractor(s) as well as completed over the past three (3) years. The Evaluation/Selection Review Committee will consider these additional references and may contact each of these sources.

c. Technical Approach and work plan that indicates how the proposer plans to address the purpose, objectives and deliverables, within the timeframes as stated in this RFP.
   - A procedure for reporting the status of the project, including work completed.
   - A proposal for how coordination will occur and how information will be shared with MHAS
   - A chart indicating the names of staff and staff hours/activities/tasks linked to the responsibility of each of those individuals involved in each deliverable of the project
   - Samples of previous related projects

d. Personnel Qualifications
   - Must include names, resumes, education, and experience of personnel listed in the table of organization/personnel chart for this project (including any subcontractors), and fully explain how their education and experience is relevant to the sections of this RFP.
   - MHAS shall require a clause in the resulting contract regarding key personnel that any person identified as critical to the success of the project may not be removed without reasonable notice to MHAS.
   - One Project Manager shall be named on behalf of the proposer. All correspondence shall be directed through this named individual.

B. Cost Proposal

The cost proposal must indicate the total cost for the entire project and a separate cost breakdown for state fiscal year 2021 for the following elements.

- Cost for Lotus Notes Application, Database, and Support for 175 User Licenses
- Complete the Lotus Notes/Domino Server software upgrades and Sever reduction installation onto a Windows Server 2019, within 2hrs
- Complete the Data Migration from the Windows Server 2008 to a Windows Server 2019, within 2hrs
- IST Test must meet a 97% pass rate, with no Priority 1 or 2 issues
- UAT Test must meet a 100% pass rate, with no Priority 3 issues

Travel cost should be encompassed within the cost of the deliverables. Travel is not to be listed separately. For purposes of this RFP, travel includes all modes of transportation (airfare, tax, car rentals, etc.), lodging expenses, meals, and cost of communications by phone, mail, e-mail, or fax.

III. PROPOSAL SUBMITTAL

Proposals must be submitted in the following manner:

- **Proposals must be submitted via e-mail by no later than 4/12/2021 at 2:00 pm EST to OhioMHASBidOpportunity@mha.ohio.gov.**

- Subject of email should be "MHA17375 Lotus Notes"
- All pages must be numbered consecutively using the format "Page [#] of [total number of pages]" (e.g., Page 2 of 20).
- Standard Affirmation and Disclosure form completed and submit with proposal
- Contractor Information form completed and submit with proposal
- Personal Service Contract form completed and submit with proposal

No proposals or corrections/additions to submitted proposals will be accepted after the Proposal Due Date and time. Proposals that are submitted after the Proposal Due Date and time will not be scored.

Proposals that are not submitted in the format requested will not be scored. Proposals that do not contain all of the required information will not be scored.

All costs incurred in the preparation of the Proposal shall be borne by the Proposer alone, and MHAS shall not contribute, in any way, to the cost of the preparation of the Proposal.

Any and all documents developed by the Proposer during the course of this project will be provided to MHAS upon request and will become the property of MHAS, and the Proposer shall not assert any claims arising under copyright or otherwise inconsistent with the transfer of ownership of such documents.

All information submitted by the Proposer will be considered to be public information unless the proposer specifically demonstrates, in writing, which information it considers to be proprietary. "Proprietary information" is information which, if made public, would put the proposer at a disadvantage in the market place and trade in which the proposer is a part. Consequently, an assertion of "proprietary" information must be clearly identified and the basis of the assertion must be included. It is not adequate for the bidder to simply state that disclosure of the information will put it at a disadvantage in the market place. MHAS will make the final decision as to whether information is "public" or "proprietary".

MHAS reserves the right to:

- Accept or reject any and all Proposals and/or bids if MHAS determines that it is in the best interests of the State to do so.
- Rebid this RFP, requesting new Proposals from qualified firms.
- Waive or modify minor irregularities in Proposals received.
- Negotiate with Proposer(s), within the requirements of this RFP, to best serve the interests of the State of Ohio.
- Require the submission of modifications or additions to Proposals as a condition of further participation in the selection process.
- Fund any Proposal in full or in part; any assignments of work by MHAS under the scope of this RFP will be made dependent on need and the availability of adequate, specific funding.
- Not make an award at the end of the evaluation process; this RFP is not to be interpreted or construed to guarantee that one or more Proposers submitting responses will be awarded contracts.
- Adjust the RFP Calendar of Event dates for whatever reason it deems appropriate.
- Contact Proposer to clarify any portion of the Proposer's submittal.

If, during the review process, MHAS determines that it is necessary to make further distinctions between certain Proposers, MHAS may request certain selected Proposers to interview or make

a presentation to staff and reviewers. The Proposer shall bear the cost of travel to any scheduled interview.

In accordance with federal and state statutes and MHAS policy, no person shall be excluded from participation or subject to discrimination in the RFP process on the basis of race, color, age, sex, national origin, military status, religion, or disability.

IV. INQUIRIES

From the issuance date of this RFP, until a contract is awarded to a proposer, there may not be communications concerning the RFP between any supplier who expects to submit a proposal and any employee of MHAS involved in the issuing of the RFP. The only exception is provided through the submission of written requests for clarification/interpretation via the state procurement website during the inquiry period.

Prospective Proposers may make inquiries or seek clarifications regarding this RFP any time during the inquiry period listed in the RFP Calendar of Events. To make an inquiry, prospective Proposers must use the following process:

1. Access the State Procurement web site at http://www.procure.ohio.gov.
2. From the Navigation Bar at the top, select “for Suppliers”.
3. Under the title “Bid Opportunities”, select “All Opportunities”.
4. Enter the RFP Number found on Page 1 of this document as the “Document/Bid Number”.
5. Click the “Search” button.
6. Select this RFP.
7. On the document information page, click the “Submit Inquiry” button.
8. On the document inquiry page, complete the required “Personal Information” section by providing the following:
    a. First and last name of the prospective Proposer’s representative who is responsible for the inquiry;
    b. Name/Company/Business of the prospective Proposer;
    c. Representative’s business phone number; and
    d. Representative’s e-mail address.
9. Type the inquiry in the space provided, making certain to include the following:
    a. A reference to the relevant part of this RFP;
    b. The heading for the provision under question; and
    c. The page number of the RFP where the provision can be found.
    d. Enter the Security Number.
10. Click the “Submit” button.

Prospective Proposers submitting inquiries will receive an immediate acknowledgement by e-mail that their inquiry has been received. **The prospective Proposer who submitted the inquiry will not receive an e-mail response to the question, but will need to view the response on the State Procurement web site where it will be posted for viewing by all prospective Proposers.**

Prospective Proposers may view inquiries using the following process:

1. Access the State Procurement web site at http://www.procure.ohio.gov.
2. From the Navigation Bar at the top, select “for Suppliers”.
3. Under the title “Bid Opportunities”, select “All Opportunities”.
4. Enter the RFP Number found on Page 1 of this document as the “Document/Bid Number”.
5. Click the “Search” button.
6. Select this RFP.
7. On the document information page, click the “View Q & A” button to display all inquiries with responses submitted to date.

MHAS will try to respond to all properly posed inquiries within 48 hours, excluding weekends and state holidays. MHAS will not respond to any inquiries received after 8:00 a.m. on 4/10/2021. Prospective Proposers who attempt to seek information or clarifications verbally will be directed to reduce their questions to writing in accordance with the terms of this RFP and state purchasing policy. No other form of communication is acceptable, and use of any other form of communication or any attempt to communicate with MHAS staff or any other agency of the State to discuss this RFP may result in the Proposer being deemed ineligible.

PART FOUR: EVALUATION OF PROPOSALS

I. EVALUATION PROCESS

MHAS's evaluation process of responses submitted to this request may consist of up to four distinct phases:

1. MHAS's initial review of all proposals for timely submission;
2. An evaluation committee review of the proposals for defects and scoring;
3. MHAS's request for more information (clarifications, interviews, presentations, and/or demonstrations); and,
4. Negotiations or best offer requests.

At its sole discretion, MHAS will determine whether phases three and/or four are necessary under this RFP, reserving for itself the ability to eliminate or add phases three or four at any time during the evaluation process. MHAS may add or remove sub-phases to phases 2 through 4 at any time if MHAS believes doing so will improve the evaluation process.

II. PROPOSAL EVALUATION CRITERIA

In the proposal evaluation phase, MHAS staff or reviewers selected by MHAS (the committee) will rate the proposals submitted in response to this RFP based on the following criteria and weight assigned to each criterion.

Evaluation Criteria	Weight	Rating	Extended Score
Complete the Lotus Notes/Domino Server software upgrades and Sever reduction installation onto a Windows Server 2019, within 2hrs	5		
Complete the Data Migration from a Windows Server 2008 to a Windows Server 2019, within 2hrs	5		
IST Test must meet a 97% pass rate, with no Priority 1 or 2 issues	4		
UAT Test must meet a 100% pass rate, with no Priority 3 issues	4		
Provide remote Go Live Support if required	4		
Provide a 30-day warranty for installation related to the Lotus Notes Application, Database and Data Migration work.	4		
Cost for Lotus Notes Application, Database, and Support for 175 User Licenses.	5		
		Total:	**155**

III. SCORING

Each proposal will be scored, and numerical technical point values will be assigned according to the criteria listed below. The scale (0-5) will be used to rate each Proposal response to the RFP on the technical evaluation sections. The Ohio Department of Mental Health and Addiction Services will score the Proposals responses by multiplying the score received in each category by its assigned weight and adding all categories together for the Offeror's total technical score.

RATINGS DEFINED:

Rating	Definition	Description of Definition
0 Points	Does Not Meet	Response does not comply substantially with requirements or is not provided.
1 Point	Weak	Response was poor related to meeting the objectives.
2 Points	Below Average	Response indicates the objectives will not be completely met or at a level that will be below average.
3 Points	Meets	Response generally meets the objectives.
4 Points	Above Average	Response indicates the objectives will be exceeded.
5 Points	Strong	Response significantly exceeds objectives in ways that provide tangible benefits or meets objectives and contains at least one enhancing feature that provides significant benefits.

The minimum acceptable score to award a contract will be: _85_

PART FIVE: CONTRACT AWARD

I. CONTRACTUAL REQUIREMENTS

Any contract(s) resulting from this issuance of this RFP are subject to the terms and conditions as provided in the personal services contract. The information contained in the RFP and in the proposal submitted by the selected contractor shall be considered part of the contract.

Payments for any and all services provided pursuant to the contract are contingent upon the availability of state and federal funds.

All aspects of the contract apply equally to work performed by any and all subcontractors.

The Contractor, and any subcontractor(s), will not use or disclose any information made available to them for any purpose other than to fulfill the contractual duties specified in the RFP. The Contractor, and any subcontractor(s), agrees to be bound by the same standards of confidentiality including federal and state statutory and regulatory requirements that apply to the employees of MHAS and the State of Ohio.

Before a contract can be awarded, an Affirmative Action Program Verification Form must be completed using the Ohio Business Gateway Electronic filing website (https://ohiobusinessgateway.ohio.gov). Contractor must have an approved Affirmative Action plan recorded with the State of Ohio Department of Administrative Services.

II. CONTRACT AWARD PROCESS

It is MHAS's intention to award one or more contract(s) under the scope of this RFP and as based on the RFP Calendar of Events schedule, so long as MHAS determines that doing so is in the State's best interests and MHAS has not otherwise changed the award date.

Any award decision by MHAS under this RFP is final. After MHAS makes its decision under this RFP, all Contractors will be notified (in writing or by phone, at MHAS's discretion) of the final evaluation and determination as to their Proposals.

MHAS will issue a notice of contract award to the selected Contractor(s), and finalized contract terms and conditions will be forwarded for signature. Contract will include RFP and attachments and the Contractor's accepted proposal. Once executed copies of the contract are submitted by the Contractor(s), and pending any further approvals that may be required (e.g., State Controlling Board), MHAS will fully execute the contract.

Once the contract is fully executed, MHAS will issue a purchase order (PO). MHAS will issue to the Contractor(s) one (1) copy of the signed instrument and one (1) copy of the PO for its/their files.

Unless otherwise negotiated and included in the executed contract/scope of work, the selected contractor(s) shall be bound by all outlined services, policies and procedures as contained in the contractor's submitted and evaluated proposal.

Contractor may commence work upon receipt of a state issued purchase order.

The selected contractor(s) shall be compensated based on deliverables listed in the RFP. The personal services contract issued will further specify the timelines for completion of each deliverable and payment structure.

III. NUMBER OF AWARDS

It is MHAS's intention to award one or more contract(s) depending on programs' needs and the fit of the Contractor(s) to the scope of this RFP.

IV. FUNDING APPROVAL THRESHOLD

In the event that contractual expenditures with the selected Contractor(s) will exceed $50,000 in spending under any contract that results from this RFP, or that otherwise exceed $50,000 in aggregate spending across all contracts between the contractor and MHAS, the contract will be subject to the approval of the State of Ohio Controlling Board.

Appendix 1:

Executive Order 2019-12D

Governing the Expenditure of Public Funds for Offshore Services

No Contract Funds May be Spent Offshore

Executive Order 2019-12D "Governing the Expenditure of Public Funds for Offshore Services" prohibits the use of any public funds within the control of an executive agency to purchase services which will be performed outside of the United States. The Executive Order can be found at the following website:

https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders/2019-12d

To be considered by the MHAS, a bid response must be accompanied by an Affirmation and Disclosure in the form attached to this RFP.

STANDARD AFFIRMATION AND DISCLOSURE FORM -EXECUTIVE ORDER 2019-12D

Governing the Expenditure of Public Funds on Offshore Services

By the signature affixed hereto, Contractor affirms, understands and will abide by the requirements of Executive Order 2019-12D. Both Contractor and any of its subcontractors shall perform no services under any contract with the Department of Developmental Disabilities outside of the United States.

The Contractor shall provide all the name(s) and location(s) where services under any contract with the Department of Developmental Disabilities will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Contractor to sanctions. If the Contractor will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Name/Principal location of Contractor:

_____

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

2. Name/Principal location of subcontractor(s):

_____

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

_____

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

3. Location(s) where services will be performed by Contractor or by subcontractors if different from principal location(s):

_____ _____

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

4. Location where state data will be stored, accessed, tested, maintained or backed-up, by Contractor or subcontractors if different from principal location(s):

_____ _____

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

Contractor affirms that Contractor and all subcontractors shall immediately disclose to the Department of Developmental Disabilities any change or shift in location of services performed by Contractor or subcontractors after execution of any Contract with the Department. On behalf of the Contractor, 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 Department and is incorporated therein.

By: _____ _____

Contractor Signature **Printed Name and Title**

Date: _____

Appendix 2:

Contractor Information Form

The Contractor Information Form must be filled out and returned with a bid response.

CONTRACTOR INFORMATION FORM

THIS FORM MUST BE SUBMITTED WITH YOUR PROPOSAL

CONTRACTOR NAME: _____

STREET ADDRESS: _____

CITY: _____ **STATE:** _____ **ZIP CODE:** _____

AUTHORIZED CONTACT NAME: _____

PHONE NUMBER: _____ **EMAIL:** _____

1. **Identify all of contracts currently with the State of Ohio (including MHAS).**

   Total # of Contracts: _____

   State Agency: _____ Amount: _____

   Contracted Services: _____

   Duration of Contract: _____

   (Attach additional sheets if necessary.)

2. **Provide current employee information on both a nationwide basis (including Ohio), and Ohio's based operations.**

	NATIONWIDE	**OHIO**
Total # of Employees:	_____	_____
Percent of Women:	_____	_____
Percent of Minorities:	_____	_____

3. **Provide OAKS Supplier ID or Tax Identification Number:** _____

4. **If your billing address is different than mailing address above, please provide below:**

   Contractor Name: _____

   Street Address: _____

   City: _____ State: _____ Zip Code: _____

_____ _____

Authorized Signature **Date**

AGREEMENT
BETWEEN THE
OHIO DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES
AND

THIS AGREEMENT is between the Ohio Department of Mental Health and Addiction Services (hereinafter the "OhioMHAS"), 30 E. Broad St. Columbus, Ohio 43215, and [Name of Contractor] (hereinafter "Contractor"), .

The parties agree as follows:

I. NATURE OF AGREEMENT

A. Contractor shall be employed as an independent contractor, to fulfill the terms of this Agreement and to act as a contractor to OhioMHAS. It is specifically understood that the nature of the services to be rendered under this Agreement are of such a personal nature that OhioMHAS is the sole judge of the adequacy of such services.

B. OhioMHAS enters into this Agreement in reliance upon Contractor's representations that it has the necessary expertise and experience to perform its obligations hereunder, and Contractor warrants that it does possess the necessary expertise and experience.

C. Contractor shall perform the services to be rendered under this Agreement and OhioMHAS shall not hire, supervise, or pay any assistants to Contractor in its performance of services under this Agreement.

II. SCOPE OF WORK

A. Contractor shall perform the services (the "Work") set forth in Exhibit 1, Scope of Work, attached hereto and made a part hereof.

B. Contractor shall, prior to undertaking any work, complete the following (select all that apply):

☐ Contractor who will be undertaking work at an OhioMHAS facility, or any personnel employed by the contractor who will be undertaking work at an OhioMHAS facility, shall, at the Contractor's expense, undergo a background investigation in the same manner as set forth in Ohio Administrative Code 5122-7-21(E)(1)(e). If the background investigation reveals a conviction or guilty plea that would disqualify an employment candidate according to Ohio Administrative Code 5122-7-21(D), the Contractor must immediately provide new personnel or OhioMHAS may unilaterally terminate this contract.

☐ Contractor who will be undertaking work at an OhioMHAS facility, or any personnel employed by the contractor who will be undertaking work at an OhioMHAS facility, shall provide results of a negative tuberculosis test conducted within six months prior to the contractor or employee beginning work at the OhioMHAS facility.

III. TIME OF PERFORMANCE

A. The Work shall be commenced on or after the date of an approved purchase order.

B. The Work shall be concluded on or before June 30, 2021, and this Agreement shall terminate on the earlier to occur of: (i) the date on which the Work is completed to the satisfaction of OhioMHAS or (ii) the date on which this Agreement is terminated as provided in Article VI, Termination of Contractor's Services.

C. The State Agency may renew this Agreement for an additional term of N/A on the same terms and conditions by giving written notice prior to expiration. As the current General Assembly cannot commit a future General Assembly to expenditure, this Agreement and any renewal shall in any event expire no later than June 30, 2021.

D. It is expressly agreed by the parties that none of the rights, duties, and obligations herein shall be binding on either party if award of this Agreement would be contrary to the terms of Ohio Revised Code ("R.C.") 3517.13, 127.16 or Chapter 102.

IV. COMPENSATION

A. OhioMHAS shall pay Contractor no more than N/A for the Work.

B. The total amount due shall be computed according to the following cost schedule (lump sum for work produced, installment payments on a schedule, hourly pay, etc):

The total of the contract and compensation schedule will be determined upon bid reviewals.

C. Travel – (choose one)

☒ No Travel - Contractor shall not be separately reimbursed for travel, lodging or any other expenses incurred in the performance of the Work.

☐ Travel Reimbursement - Contractor shall be reimbursed for the Contractor's reasonable, actual and necessary travel, lodging, and other travel-related expenses incurred in the performance of the Work to the extent that such reimbursement is in the best interest of the state.

1. Only travel expenses which are pre-approved by OhioMHAS will be reimbursed.

2. Travel expenses shall be reimbursed under the same rules and conditions that apply to state employees under Ohio Adm.Code 126-1-02, pursuant to the Ohio Office of Budget and Management ("OBM") Travel Policy, attached as Exhibit 2.

3. If it is not possible to follow the OBM Travel Policy, with prior approval of OhioMHAS, Contractor shall be reimbursed pursuant to the federal rates for reimbursement in the Continental United States.

4. Meals shall not be reimbursed unless overnight travel is both critical and essential.

D. Contractor must receive a purchase order from OhioMHAS prior to filling an order or performing any of the Work.

E. After Contractor receives a purchase order, Contractor shall submit an invoice for the Work performed consistent with this Article IV, Compensation. Each invoice shall contain an itemization of the Work performed, including dates the Work was performed and total hours worked, if required by Paragraph B.1., above, the location or address where the Work was performed, and the sum due at that time pursuant to this Agreement. All invoices shall contain Contractor's name and address and shall reference OhioMHAS and list the billing address as [Billing Address], Attn: . All invoices must be submitted no later than sixty days after the Work performed. After receipt and approval by OhioMHAS of a proper invoice, as defined by Ohio Adm.Code 126-3-01(A)(5), payment will be made pursuant to Ohio Adm.Code 126-3-01. Unless otherwise directed by OhioMHAS, invoices should be directed via email to: .

F. In the event that any customer of Contractor negotiates a lower fee structure for the Work or comparable services, Contractor shall promptly notify OhioMHAS and shall extend the lower negotiated rate to OhioMHAS retroactively to the first date the lower rate was offered to another customer.

V. CERTIFICATION OF FUNDS

A. It is expressly understood and agreed by the parties that none of the rights, duties, and obligations described in this Agreement shall be binding on either party until all relevant statutory provisions of the Ohio Revised Code, including, but not limited to, R.C. 126.07, have been complied with, and until such time as all necessary funds are available or encumbered and, when required, such expenditure of funds is approved by the Controlling Board of the State of Ohio, or in the event that grant funds are used, until such time that OhioMHAS gives Contractor written notice that such funds have been made available to OhioMHAS by OhioMHAS's funding source.

VI. TERMINATION OF CONTRACTOR'S SERVICES

A. OhioMHAS may, at any time prior to completion of the Work, suspend or terminate this Agreement with or without cause by giving written notice to Contractor.

B. In the event that the Work includes divisible services, OhioMHAS may, at any time prior to completion of the Work, by giving written notice to Contractor, suspend or terminate any one or more such portions of the Work.

C. Contractor, upon receipt of notice of suspension or termination, shall cease work on the suspended or terminated activities under this Agreement, suspend or terminate all subcontracts relating to the suspended or terminated activities, take all necessary or appropriate steps to limit disbursements and minimize costs, and, if requested by OhioMHAS, furnish a report, as of the date Contractor receives notice of suspension or termination, describing the status of all Work, including, without limitation, results, conclusions resulting there from, and any other matters OhioMHAS requires.

D. Contractor shall be paid for services rendered up to the date Contractor received notice of suspension or termination, less any payments previously made, provided Contractor has supported such payments with detailed factual data containing Work performed and hours worked. In the event of suspension or termination, any payments made by OhioMHAS for which Contractor has not rendered services shall be refunded.

E. In the event this Agreement is terminated prior to completion of the Work, Contractor shall deliver to OhioMHAS all work products and documents which have been prepared by Contractor in the course of performing the Work. All such materials shall become, and remain the property of, OhioMHAS, to be used in such manner and for such purpose as OhioMHAS may choose.

F. Contractor agrees to waive any right to, and shall make no claim for, additional compensation against OhioMHAS by reason of any suspension or termination.

G. Contractor may terminate this Agreement upon sixty (60) days' prior written notice to OhioMHAS.

H. If the Contractor fails to perform any of the requirements of this contract, or is in violation of a specific provision of this contract, OhioMHAS may provide the Contractor written notice of the failure to perform or the violation and may provide a specified period to cure any and all defaults under this contract. During the cure period, the Contractor shall incur only those obligations or expenditures which are necessary to enable the Contractor to continue its operation and achieve compliance as set forth in the notice. Should the Contractor fail to comply within OhioMHAS's cure period, the Contractor shall be held in default of this contract and the contract shall terminate at the end of the cure period.

VII. RELATIONSHIP OF PARTIES

A. Contractor shall be responsible for all of its own business expenses, including, but not limited to, computers, email and internet access, software, phone service and office space. Contractor will also be responsible for all licenses, permits, employees' wages and salaries, insurance of every type and description, and all business and personal taxes, including income and Social Security taxes and contributions for Workers' Compensation and Unemployment Compensation coverage, if any.

B. While Contractor shall be required to render services described hereunder for OhioMHAS during the term of this Agreement, nothing herein shall be construed to imply, by reason of Contractor's engagement hereunder as an independent contractor, that OhioMHAS shall have or may exercise any right of control over Contractor with regard to the manner or method of Contractor's performance of services hereunder.

C. Except as expressly provided herein, neither party shall have the right to bind or obligate the other party in any manner without the other party's prior written consent.

D. It is fully understood and agreed that Contractor is an independent contractor and neither Contractor nor its personnel shall at any time, or for any purpose, be considered agents, servants, or employees of OhioMHAS. Unless Contractor is another State of Ohio entity or a participant in the Ohio Public Employees Retirement System (OPERS), Contractor and its personnel shall not be considered agents, servants, or employees of the State of Ohio, or public employees for the purpose of OPERS benefits.

E. Unless Contractor is a "business entity" as that term is defined in R.C. 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business"), Contractor shall have any individual performing services under this Agreement complete and submit to OhioMHAS the Independent Contractor/Worker Acknowledgement form found at https://www.opers.org/forms-archive/PEDACKN.pdf. This paragraph is not applicable to OPERS member employers.

F. Contractor's failure to complete and submit the Independent Contractor/Worker Acknowledgement form linked in Paragraph VII(E) at the time Contractor executes this Agreement shall serve as Contractor's certification that Contractor is a "business entity" as that term is defined in R.C. 145.037.

G. Contractor declares that it has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage that is required in the normal course of business.

H. Contractor agrees that it does not have any authority to sign agreements, notes, and/or obligations or to make purchases and/or dispose of property for, or on behalf of, the State of Ohio or OhioMHAS.

I. Contractor agrees that while operating in an OhioMHAS facility, the Contractor and/or any employee or subcontractor of the Contractor, shall follow all applicable rules and regulations for that facility.

VIII. RECORD KEEPING

A. The Contractor must keep all financial records in a manner consistent with generally accepted accounting principles. Additionally, the Contractor must keep separate business records for this project, including records of disbursements and obligations incurred that must be supported by contracts, invoices, vouchers and other data as appropriate.

B. During the period covered by this contract and until the expiration of three (3) years after final payment under this contract, the Contractor agrees to provide the State, its duly authorized representatives or any person, agency or instrumentality providing financial support to the work undertaken hereunder, with access to and the right to examine any books, documents, papers and records of the Contractor involving transactions related to this contract.

C. The Contractor shall, for each subcontract in excess of two thousand five hundred dollars ($2,500), require its subcontractors to agree to the same provisions. The Contractor may not artificially divide contracts with its subcontractors to avoid requiring subcontractors to agree to this provision.

D. The Contractor must provide access to the requested records no later than five (5) business days after the request by the State or any party with audit rights. If an audit reveals any material deviation from the contract requirements, and misrepresentations or any overcharge to the State or any other provider of funds for the contract, the State or other party will be entitled to recover damages, as well as the cost of the audit.

E. If this contract or the combination of all other contracts with the Contractor exceeds ten-thousand dollars ($10,000) over a twelve (12) month period, the Contractor agrees to allow federal government access to the contracts and books, documents, and records needed to verify the Contractor's and/or subcontractor's costs.

F. The Contractor must comply with any direction from OhioMHAS to preserve documents and information, in both electronic and paper form, and to suspend any scheduled destruction of such documents and information.

IX. RELATED AGREEMENTS

A. All Work is to be performed by Contractor, who may subcontract without OhioMHAS's approval for the purchase of articles, supplies, components, or special mechanical services that do not involve the type of work or services described in Exhibit 1, Scope of Work, but which are required for satisfactory completion of the Work.

1. Contractor shall not enter into subcontracts related to the Scope of Work without prior written approval by OhioMHAS. All work subcontracted shall be at Contractor's expense.

2. Contractor shall furnish to OhioMHAS a list of all subcontractors; their addresses; tax identification numbers; current licensure, certification, or accreditation, incuding any renewal or re-issuance thereof; and the dollar amount of each subcontract.

B. Contractor shall bind its subcontractors to the terms of this Agreement, so far as applicable to the work of the subcontractor, and shall not agree to any provision which seeks to bind OhioMHAS to terms inconsistent with, or at variance from, this Agreement.

C. Contractor warrants that it has not entered into, nor shall it enter into, other agreements, without prior written approval of OhioMHAS, to perform substantially identical work for the State of Ohio such that the Work duplicates the work called for by the other agreements.

X. RIGHTS IN DATA AND COPYRIGHTS/PUBLIC USE

A. OhioMHAS shall have unrestricted authority to reproduce, distribute and use (in whole or in part) any reports, data or materials prepared by Contractor pursuant to this Agreement. No such documents or other materials produced (in whole or in part) with funds provided to Contractor by OhioMHAS shall be subject to copyright by Contractor in the United States or any other country.

B. Contractor agrees that all original works created under this Agreement shall be made freely available to the general public to the extent permitted or required by law until and unless specified otherwise by OhioMHAS. Any requests for distribution received by Contractor shall be promptly referred to OhioMHAS.

XI. CONFIDENTIALITY

A. Contractor shall not discuss or disclose any information or material obtained pursuant to its obligations under this Agreement without the prior written consent of OhioMHAS.

B. If applicable, the Contractor agrees to execute the OhioMHAS business associate and/or qualified service organization agreement, or acknowledge receipt of HIPAA/42 CFR Part 2 training by executing the OhioMHAS Assurance of Preservation of the Confidentiality and Security of Protected Health Information prior to accessing any PHI or PII relating to services rendered under this contract.

C. The Contractor agrees not to use advertising, news releases, sales promotions, or other publicity matters relating to any product or service furnished by the Contractor wherein OhioMHAS's name is mentioned, or language used from which a connection with OhioMHAS may be reasonably inferred, without the prior, written consent of OhioMHAS.

XII. CONTRACT REMEDIES

A. The Contractor is liable to OhioMHAS for all actual and direct damages caused by Contractor's default. OhioMHAS may buy substitute services from a third party for those that were to be provided by the Contractor. OhioMHAS may recover from the Contractor the costs associated with acquiring substitute services, less any expenses or costs saved by the Contractor's default.

B. If actual or direct damages are uncertain or difficult to determine, OhioMHAS may recover liquidated damages in the amount of one (1) percent of the value of the deliverable that is the subject of the default, for every day that the default is not cured by the Contractor.

XIII. LIABILITY

A. To the extent permitted by law, Contractor agrees to indemnify and to hold OhioMHAS and the State of Ohio harmless and immune from any and all claims for injury or damages arising from this Agreement which are attributable to Contractor's own actions or omissions or those of its trustees, officers, employees, subcontractors, suppliers, third party agents or joint venturers while acting under this Agreement. Such claims shall include any claims made under the Fair Labor Standards Act or under any other federal or state law involving wages, overtime or employment matters and any claims involving patents, copyrights and trademarks.

B. OhioMHAS's liability for damages, whether in contract or in tort, shall not exceed the total amount of compensation payable to the Contractor under this contract. In addition, to the extent permitted by law, the Contractor agrees that OhioMHAS and the State of Ohio and any funding source for this contract are held harmless and immune from any and all claims for injury or damages arising from this contract which are attributable to the Contractor's own actions or omissions or those of its trustee, officers, employees, subcontractors, suppliers, and other third parties while acting under this contract. Such claims shall include any claims made under the Fair Labor Standards Act or under any other federal or state law involving wages, overtime, or employment matters and any claims involving patents, copyrights and trademarks. To the extent permitted by law, Contractor agrees to bear all costs associated with defending against any such claims or legal actions when requested by OhioMHAS or the State to do so.

C. To the extent permitted by law, Contractor shall bear all costs associated with defending OhioMHAS and the State of Ohio against any such claims.

D. In no event shall either party be liable to the other party for indirect, consequential, incidental, special or punitive damages, or lost profits.

XIV. ANTITRUST ASSIGNMENT

A. Contractor assigns to OhioMHAS all State and Federal antitrust claims and causes of action that relate to all goods and services provided for in this Agreement. Additionally, the State of Ohio will not pay excess charges resulting from antitrust violations by Contractor's suppliers and subcontractors.

XV. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES

A. COMPLIANCE WITH LAWS. Contractor, in the execution of its duties and obligations under this Agreement, agrees to comply with all applicable federal, state and local laws, rules, regulations and ordinances.

B. DRUG FREE WORKPLACE. Contractor agrees to comply with all applicable federal, state and local laws regarding smoke-free and drug-free work places and shall make a good faith effort to ensure

that none of its employees or permitted subcontractors engaged in the Work purchase, transfer, use or possess illegal drugs or alcohol, or abuse prescription drugs in any way.

C. DISTRACTED DRIVING. Contractor agrees to refrain from any activities that may result in distracted driving, either when operating a state owned vehicle or operating a personally-owned vehicle while conducting business pursuant to this agreement.

D. NONDISCRIMINATION OF EMPLOYMENT. Pursuant to R.C. 125.111, OhioMHAS policy, and applicable Exectuive Orders Contractor agrees that Contractor, any subcontractor, and any person acting on behalf of Contractor or a subcontractor, shall not discriminate, by reason of race, color, religion, gender, gender identity or expression, sexual orientation, age, disability, military status, national origin, or ancestry, status as a parent during pregnancy and immediately after the birth of a child, status as a parent of a young child, status as a foster parent, or genetic information against any citizen of this state in the employment of any person qualified and available to perform the Work. Contractor further agrees that Contractor, any subcontractor, and any person acting on behalf of Contractor or a subcontractor shall not, in any manner, discriminate against, intimidate, or retaliate against any employee hired for the performance of the Work on account of race, color, religion, gender, gender identity or expression, sexual orientation, age, disability, military status, national origin, or ancestry, status as a parent during pregnancy and immediately after the birth of a child, status as a parent of a young child, status as a foster parent, or genetic information.

E. AFFIRMATIVE ACTION PROGRAM. Contractor represents that it has a written affirmative action program for the employment and effective utilization of economically disadvantaged persons pursuant to R.C. 125.111(B) and has filed an Affirmative Action Program Verification form with the Equal Employment Opportunity and Affirmative Action Unit of the Department of Administrative Services.

F. CONFLICTS OF INTEREST.

No personnel of Contractor who exercise any functions or responsibilities in connection with the review or approval of this Agreement or carrying out of any of the Work shall, prior to the completion of the Work, voluntarily acquire any personal interest, direct or indirect, which is incompatible or in conflict with the discharge and fulfillment of his or her functions and responsibilities with respect to the carrying out of the Work. Any such person who acquires an incompatible or conflicting personal interest on or after the effective date of this Agreement, or who involuntarily acquires any such incompatible or conflicting personal interest, shall immediately disclose his or her interest to OhioMHAS in writing. Thereafter, he or she shall not participate in any action affecting the Work, unless OhioMHAS shall determine in its sole discretion that, in light of the personal interest disclosed, his or her participation in any such action would not be contrary to the public interest.

G. ETHICS COMPLIANCE. Contractor represents, warrants and certifies that it and its employees engaged in the administration or performance of this Agreement are knowledgeable of and understand the Ohio Ethics and Conflict of Interest laws [ORC Chapters 102 and 2921]. Contractor further represents, warrants, and certifies that neither Contractor nor any of its employees will do any act that is inconsistent with such laws.

H. QUALIFICATIONS TO DO BUSINESS. Contractor affirms that it has all of the approvals, licenses, or other qualifications needed to conduct business in Ohio and that all are current. If at any time during the term of this Agreement Contractor, for any reason, becomes disqualified from conducting business in the State of Ohio, Contractor will immediately notify OhioMHAS in writing and will immediately cease performance of the Work.

I. CAMPAIGN CONTRIBUTIONS. Contractor hereby certifies that neither Contractor nor any of Contractor's partners, officers, directors or shareholders, nor the spouse of any such person, has made contributions in excess of the limitations specified in R.C. 3517.13.

J. FINDINGS FOR RECOVERY. Contractor warrants that it is not subject to an "unresolved" finding for recovery under R.C. 9.24.

K. DEBARMENT. Contractor represents and warrants that it is not debarred from consideration for contract awards by the Director of the Department of Administrative Services, pursuant to either R.C. 153.02 or R.C. 125.25.

L. OFFSHORE SERVICES. Contractor affirms to have read and understands Executive Order 2019-12D and shall abide by those requirements in the performance of this Agreement. Notwithstanding any other terms of this Agreement, OhioMHAS reserves the right to recover any funds paid for services the Contractor performs outside of the United States for which it did not receive a waiver. OhioMHAS does not waive any other rights and remedies provided OhioMHAS in this Agreement. The Contractor agrees to complete the attached Exhibit 3, Executive Order 2019-12D Affirmation and Disclosure Form, which is incorporated and becomes a part of this Agreement.

M. REPAYMENT. If the representations and warranties in Paragraphs J or K of this Article XV are found to be false, this Agreement is void ab initio and Contractor shall immediately repay to OhioMHAS any funds paid under this Agreement.

N. BOYCOTTING. Pursuant to R.C. 9.76(B), Contractor warrants that Contractor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the term of this Agreement.

XVI. MISCELLANEOUS

A. CONTROLLING LAW. This Agreement and the rights of the parties hereunder shall be governed, construed, and interpreted in accordance with the laws of the State of Ohio, without regard to choice of law provisions.

B. WAIVER. A waiver by any party of any breach or default by the other party under this Agreement shall not constitute a continuing waiver by such party of any subsequent act in breach of or in default hereunder.

C. SURVIVAL. The provisions of Articles IV, VI, VII(G), VIII, X, XI, XIII, XIV and XV(M) hereof shall survive the termination or expiration of this Agreement.

D. SUCCESSORS AND ASSIGNS. Neither this Agreement nor any rights, duties or obligations hereunder may be assigned or transferred in whole or in part by Contractor, without the prior written consent of OhioMHAS.

E. NOTICES. Except to the extent expressly provided otherwise herein, all notices, consents and communications required hereunder (each, a "Notice") shall be in writing and shall be deemed to have been properly given when: 1) hand delivered with delivery acknowledged in writing; 2) sent by U.S. Certified mail, return receipt requested, postage prepaid; 3) sent by overnight delivery service (Fed Ex, UPS, etc.) with receipt; or 4) sent by fax or email. Notices shall be deemed given upon receipt thereof, and shall be sent to the addresses first set forth above. Notwithstanding the foregoing, notices sent by fax or email shall be effectively given only upon acknowledgement of receipt by the receiving party. Any party may change its address for receipt of Notices upon notice to the other party. If delivery

cannot be made at any address designated for Notices, a Notice shall be deemed given on the date on which delivery at such address is attempted.

F. CONFLICT. In the event of any conflict between the terms and provisions of the body of this Agreement and any exhibit hereto, the terms and provisions of the body of this Agreement shall control.

G. HEADINGS. The headings in this Agreement have been inserted for convenient reference only and shall not be considered in any questions of interpretation or construction of this Agreement.

H. SEVERABILITY. The provisions of this Agreement are severable and independent, and if any such provision shall be determined to be unenforceable in whole or in part, the remaining provisions and any partially enforceable provision shall, to the extent enforceable in any jurisdiction, nevertheless be binding and enforceable.

I. ENTIRE AGREEMENT. This Agreement contains the entire agreement between the parties hereto as to the subject matter herein and shall not be modified, assigned or supplemented, or any rights herein waived, unless specifically agreed upon in writing by the parties hereto. This Agreement supersedes any and all previous agreements, whether written or oral, between the parties.

J. EXECUTION. This Agreement is not binding upon OhioMHAS unless executed in full, and is effective as of date/the last date of signature by OhioMHAS.

K. COUNTERPARTS. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, and all of which shall constitute but one and the same instrument.

L. FACSIMILE SIGNATURES. Any party hereto may deliver a copy of its counterpart signature page to this Agreement via fax or e-mail. Each party hereto shall be entitled to rely upon a facsimile signature of any other party delivered in such a manner as if such signature were an original.

M. CONTRACT CONSTRUCTION: This contract will be construed in accordance with the plain meaning of its language and neither for nor against the drafting party.

N. ACCREDITATION STANDARDS: The services to be performed under this contract shall meet standards required by the Joint Commission, Centers for Medicaid & Medicare Services or other accrediting or certifying organizations, as appropriate.

O. PUBLICITY: The Contractor will not advertise that it is doing business with the State or use this contract as a marketing or sales tool without prior, written consent of the State.

P. FORCE MAJEURE: If OhioMHAS or the Contractor is unable to perform any part of its obligations under this contract by reason of force majeure, the party will be excused from its obligations, to the extent that its performance is prevented by force majeure for the duration of the event. The party must remedy with all reasonable dispatch the cause preventing it from carrying out its obligations under the contract. The term "force majeure" means without limitation: acts of God such as epidemics; lightning; earthquakes; fires; storms; hurricanes; tornadoes; floods; washouts; droughts; other severe weather; explosions; restraint of government and people; war; strikes; and other like events; or any cause that could not be reasonably foreseen in the exercise of ordinary care, and that is beyond the reasonable control of the party.

Q. STRICT PERFORMANCE: The failure of either party at any time to demand strict performance by the other party of any of the terms of this contract will not be construed as a waiver of any such term, and either party may at any time demand strict and complete performance by the other party.

R. TAXES: The Contractor affirms that it is not delinquent in the payment of any applicable federal, state, and local taxes and agrees to comply with all applicable federal, state and local laws in the performance of the work hereunder.

S. WORKERS' COMPENSATION: The Contractor must maintain workers' compensation insurance as required by Ohio law and the laws of any other state where work is performed under this contract. The Contractor must submit proof of workers' compensation insurance upon request.

T. The Contractor accepts full responsibility for payment of all taxes, including and without limitation, unemployment compensation, insurance premiums, all income tax deductions, social security deductions, and any and all other taxes or payroll deductions required for all employees engaged by the Contractor in the performance of the work authorized by this Contract. OhioMHAS and the State of Ohio shall not be liable for any taxes under this contract.

(remainder of page intentionally left blank)

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

CONTRACTOR

By: _____

Name: _____

Title: _____

Date: _____

STATE OF OHIO
Ohio Department of Mental Health and Addiction Services

Director/CEO:

_____

Name: _____

Title: _____

Date: _____

PROCUREMENT OFFICER

By: _____

Name: _____

Title: _____

Date: _____

Approval as to form:

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 1
Scope of Work

- Install Lotus Notes Application onto a Windows 2019 Server
- Successful migrate database information onto a Window 2019 Server
- Ensure integration testing (IST) meets the success criterion
- Provide system configuration information to MHAS OIS System Engineering
- Provide a 30-day Application and Data Migration installation warranty
- Provide remote Go Live Support if required.

EXHIBIT 2
Ohio Office of Budget and Management Travel Policy

126-1-02 Rates and requirements for reimbursement of travel expenses of state agents.

(A) Definitions

(1) "Compensation" means payment for services rendered, whether made on an hourly, per diem, salaried, or fee basis but does not include reimbursement of travel expenses.

(2) "Headquarters" means the office address at which a state agent has his/her primary work assignment.

(3) "Continental U.S. travel" means travel within the Continental United States, including the lower forty-eight states, excluding Hawaii and Alaska.

(4) "International travel" means travel outside of the Continental United States, including Hawaii and Alaska.

(5) "Reimbursable travel expenses" means those expenses which are actually incurred as a necessary part of approved travel. In addition to lodging, meals, per diem, and mileage, it includes:

(a) Miscellaneous transportation expenses such as parking charges, road tolls, and other reasonably incurred transportation expenses directly related to authorized travel, provided such expenses are listed separately on a state agent's travel expense reimbursement request;

(b) Commercial transportation expenses paid by the state agent such as taxi cabs, automobile rental , airfare, ferries, subways, bus, trains, and other commercial transportation providers;

(c) Registration fees paid by the state agent for professional events such as conferences, seminars, and meetings ;

(d) Miscellaneous business expenses such as telephone, facsimile, internet, and other similar charges paid by the state agent for official state business;

(e) Miscellaneous living expenses such as laundry, dry cleaning, personal telephone calls, and postage .

(6) "State agency" means every organized body, office, or agency established by the laws of the state for the exercise of any function of state government which uses money that has been appropriated to it directly, but does not include the general assembly,supreme court, court of appeals, court of claims, any agency of these, or any state university or college as defined in division (A)(1) of section 3345.12 of the Revised Code .

(7) "State agent" means any officer, member, or employee of a state agency whose compensation is paid, in whole or in part, from state funds but does not include any volunteer serving without compensation:

(8) "Travel at state expense" means travel expenses which are paid from moneys appropriated directly to a state agency by the general assembly, but does not include travel by a state agent where expenses are paid pursuant to rule 102-3-08 of the Administrative Code.

(9) "Receipt" means the original document provided by a service provider or merchant that indicates the merchant's name, date of purchase, transaction amount, and line item detail identifying the service or goods provided.

(10) "Supporting documentation" means documents that validate expense claims to include, but not limited to the following:

(a) Conference material provided by the conference organizer.

(b) Formal meeting agenda provided by the meeting organizer.

(c) Currency exchange rate as evidenced by a foreign currency exchange receipt, bank or credit card statement, or the exchange rate issued by an authoritative source such as "OANDA" (http://www.oanda.com/currency/historical-rates/) for the travel period. Expenses shall be recorded on the travel expense report in U.S. dollars. Reimbursements authorized by this rule will be made in U.S. dollars. The original itemized receipt and the currency exchange rate documentation described in this rule is required.

(d) State agency authorizations.

(11) "Conference" means a prearranged gathering with a formal agenda, for consultation or exchange of information or discussion that benefits the state, such as seminars, meetings, and other professional events.

(12) "Paid travel status" means the designation given to a state agent who is traveling on behalf of the state and is in an active pay status.

(B) Authority for travel and reimbursement

(1) Authority for travel

All state agents traveling at state expense or on paid travel status must be authorized prior to travel by the head of a state agency or his/her designee. Travel may be authorized only for official state business and only if the state agency has the financial resources to reimburse the state agent for travel expenses. State agents who are traveling at state expense or who are on paid travel status must, at all times, use prudent judgment in the use of state resources, incurring only those expenses necessary to carry out the official business of the state.

(2) Reporting requirements

(a) A state agent who has traveled at state expense and is requesting reimbursement by a state agency of his/her travel expenses shall report his/her travel expenses as prescribed by the office of budget and management. A state agent shall submit the travel expense reimbursement request within sixty days of the last date of travel. This time frame may be extended by the head of the state agency or his/her designee if mitigating circumstances exist, but in no case may this time frame exceed one hundred twenty days from the last date of travel. A completed request for travel expense reimbursement may be denied by the office of budget and management for reasons including, but not limited to, a state agent's failure to submit the request in a timely, accurate, or truthful manner.

(b) A state agent shall obtain and provide all receipts and supporting documentation required by this rule.

(c) At no time shall a state agent claim or be reimbursed more than is allowable under this rule.

(3) Approval of travel

When the head of a state agency or his/her designee approves of a state agent's travel, such action constitutes certification of the propriety of the reimbursement of such state agent's travel expenses. The head of a state agency or his/her designee may require any reasonable form of verification of an expense if he/she determines that additional verification is necessary to his/her certification of the propriety of the reimbursement or if required receipts are not available.

(4) Reimbursement of expenses

A state agent shall be reimbursed for his/her travel expenses as authorized by this rule upon approval by the head of a state agency or his/her designee. Reimbursement for travel expenses shall be via electronic funds transfer to the same bank account that a state agent has established for receipt of his/her compensation in accordance with section 124.151 of the Revised Code.

(5) Submission of receipts

As specified by the office of budget and management, original or a legible electronic copy of receipts shall be submitted to the office of budget and management.

(6) Direct payment to vendor

Instead of reimbursing a state agent for his/her travel expenses, a state agency may make direct payment to a vendor who provides travel services for the state agent. A direct payment shall comply with the applicable rates and requirements specified in this rule.

(C) Transportation expenses

The head of a state agency or his/her designee shall, subject to the discretion of the office of budget and management, determine the appropriate mode or modes of transportation to be utilized by a state agent.

(1) Travel by state-owned automobile

Travel by state-owned automobile is authorized only for state agents and for other parties who are properly designated by a state agency and endorsed onto insurance coverage through the department of administrative services. Reimbursement is authorized for incurred service expenses necessary to the efficient and safe operation of a state-owned automobile. The names of all persons traveling in the same state-owned automobile and names of their respective state agencies shall be listed on any travel expense reimbursement request.

(2) Travel by privately owned automobile

Travel by privately owned automobile is authorized only if the owner thereof is insured under a policy of liability insurance complying with the requirements of section 4509.51 of the Revised Code. Reimbursement of mileage expenses incurred on state business is authorized at a rate up to the internal revenue service's business standard mileage rate, within the discretion of the

director of the office of budget and management. The reimbursement rate for mileage expenses incurred on state business may not fall below forty-five cents per mile, unless the internal revenue service's business standard mileage rate falls below forty-five cents per mile, in which case the director may lower the reimbursement rate below forty-five cents per mile. The director of the office of budget and management will review the appropriate mileage reimbursement rate on a quarterly basis.

A state agent shall not be reimbursed for mileage commuting from his/her residence to his/her headquarters nor from his/her headquarters to his/her residence. If a state agent is required to report to a location other than his/her headquarters, the state agent will only be reimbursed for the distance from his/her residence to the alternate location less the state agent's normal commute. For example, if a state agent's normal commute from his/her residence to his/her headquarters is ten miles, and a state agent's commute from his/her residence to his/her authorized destination is thirty miles, the state agent shall only be reimbursed for twenty miles.

Travel expense reports shall indicate all intermediate destinations (i.e., specify intermediate towns and cities but not stops within a town or city) between the commencement and termination of travel as well as all vicinity mileage after arrival at destination. Reimbursement shall be made to only one of two or more state agents traveling in the same privately owned automobile, and the names of their respective state agencies shall be listed on the travel expense reimbursement request.

(3) Travel by commercial transportation

(a) Travel by commercial transportation is authorized at the lowest available rate. When any segment of travel by commercial transportation exceeds eight hours, the head of the state agency may authorize business class travel for the state agent.

(b) State funds shall not be expended to pay for unused reservations with commercial transportation unless the state agency is satisfied that failure to cancel or use the reservation was unavoidable. State agency authorization shall be required as supporting documentation.

(c) Travel within the state of Ohio by common air carrier at the lowest available rate is authorized for elected officials, directors, assistant directors, deputy directors, board and commission members, and heads of state agencies. State employees not listed in this paragraph are authorized to travel within the state of Ohio by common air carrier at the lowest available rate only if flying is more economical than other modes of travel.

(d) Reimbursement is authorized for automobile rental if automobile rental is more economical than any other mode of transportation or if the state agent's destination is not easily accessible by any other mode of transportation. The state agent must purchase liability insurance and loss damage waiver for accidents arising out of the operation or use of the automobile and include that cost in determining whether the automobile rental is the most economical mode of transportation.

(4) Required receipts for transportation expenses

Except as otherwise provided, receipts are required for all service expenses incurred in connection with the operation of state-owned automobiles, all commercial transportation expenses, and all miscellaneous transportation expenses exceeding ten dollars.

(D) Meal, incidental, and miscellaneous expenses within the Continental U.S.

(1) Restrictions and reimbursement per diem

Meals and incidental per diem for state agents is authorized only when overnight lodging is required. State agents may receive per diem for meal and incidental expenses in accordance with the per diem rates established by the U.S. general services administration (www.gsa.gov), which is based on the lodging location. Per diem is designed to offset the additional cost of travel, not to entirely pay for the state agent's meal and incidental expenses. The amount of per diem shall be adjusted on departure and return days based upon the time of departure and return. The standard meal and incidental expenses allowance is based on a full day of official travel (twenty-four hours) within the continental U.S. Where overnight lodging is required and where a state agent is on travel status for less than a full day, the meal and incidental expenses rate for the departure and return days shall be pro-rated as follows:

(a) Twenty-five per cent of the standard meal and incidental expenses allowance if the state agent is on travel status for less than six hours;

(b) Fifty per cent of the standard meal and incidental expenses allowance if the state agent is on travel status for six hours but less than twelve hours;

(c) Seventy-five per cent of the standard meal and incidental expenses allowance if the state agent is on travel status for twelve hours but less than eighteen hours;

(d) One hundred per cent of the standard meal and incidental expenses allowance if the state agent is on travel status for eighteen hours but less than twenty-four hours.

(e) Notwithstanding the restrictions provided in paragraph (D)(1) of this rule, where a state agency elects to schedule a state agent to travel out of state by air travel and schedules a return flight for the same day, meals and incidental per diem is authorized; however, the meal and incidental expenses shall be pro-rated as provided in paragraphs (D)(1)(a) to (D)(1)(d) of this rule.

(2) Incidental expenses included in the per diem allowance are listed as follows and are thus not separately reimbursable:

(a) All gratuities given to porters, baggage carriers, bellhops, hotel maids, flight attendants, ship attendants, taxi drivers, wait staff and all other services related to the hospitality industry ;

(b) Any transportation between places of lodging or business and places where meals are taken, if suitable meals cannot be obtained at the temporary lodging or business site;

(c) Mailing costs associated with filing travel reimbursement requests.

(3) A receipt shall be required for any single miscellaneous business expenses charge over ten dollars. State agents shall first use any free internet or phone services prior to incurring these expenses.

(4) If the state agent is in overnight status in the continental U.S. for more than one week, including a weekend, miscellaneous living expenses will be reimbursed when such expense is reasonable as determined by the head of the state agency or his/her designee. Receipts shall be required for all miscellaneous living expenses.

(E) Meal, incidental, and miscellaneous expenses outside the continental U.S. (international)

(1) A state agent traveling outside the continental U.S., assigned to a foreign office, or otherwise on approved international travel status, including international conferences, shall be entitled to reimbursement of meals and meal gratuities up to twenty per cent of the cost of the meal at actual

cost when such cost is reasonable as determined by the head of the state agency or his/her designee.

(2) If the state agent is in overnight international travel status for more than one week, including a weekend, miscellaneous living expenses will be reimbursed when such expense is reasonable as determined by the head of the state agency or his/her designee.

(3) Receipts shall be required for international travel expenses, which include commercial transportation, lodging, meal, meal gratuities , and miscellaneous living expenses. Currency exchange rates shall be provided as supporting documentation.

(4) A receipt shall be required for any single miscellaneous business expense charge exceeding ten dollars. State agents shall first use any free internet or phone services prior to incurring these expenses. Currency exchange rates shall be provided as supporting documentation.

(F) Lodging

(1) Continental U.S.

In accordance with the per diem rates established by the U.S. general services administration, reimbursement of expenses incurred while on official travel status within the continental U.S. is authorized per state agent per calendar day for lodging in commercial establishments . at actual cost up to the maximum allowable lodging rate for that location, plus applicable taxes on the entire room.

(2) Outside the continental U.S. (international)

Reimbursement for lodging in commercial establishments is authorized per state agent per calendar day at actual cost when such cost is reasonable as determined by the head of a state agency or his/her designee. The currency exchange rate shall be provided as supporting documentation.

(3) Receipts are required for all lodging expenses.

(4) Overnight lodging may be reimbursed only when the state agent is traveling on official state business and is either:

(a) At a location greater than forty-five miles from both the state agent's residence and headquarters, or;

(b) At a location greater than thirty miles from both the state agent's residence and headquarters for conference purposes.

(G) Conferences

Reimbursement is authorized for conference registration fees and conference expenses as follows:

(1) Registration fees

Conference registration fees may be reimbursed to the state agent, or conference registration fees may be paid directly by a state agency in advance of the event. If the registration fee includes any meals, the state agent shall not be reimbursed for those same meals under paragraphs (D) and

(E) of this rule, and any amount reimbursed to the state agent under paragraphs (D) and (E) of this rule for meals shall be adjusted accordingly.

(2) Meal and incidental

If the event includes or provides a meal, the state agent shall not be reimbursed for that same meal under paragraphs (D) and (E) of this rule. State agents shall receive per diem for any meals not provided by the event and incidentals at the rate prescribed by the U.S. general services administration.

When meals are included with registration expense, the number and type of meals must be identified by the state agent. If a meal is offered as part of the event and the state agent has medical restrictions, the state agent should make every effort to have the conference facilitate his or her needs. If the event does not honor the request, the state agent is not required to deduct the applicable meal allowance from the per diem, but must include documentation explaining the situation.

(3) Lodging

Lodging at the event site or lodging at a hotel identified in the event registration materials as one of the event hotels may be reimbursed at actual cost, provided such cost is reasonable as determined by the head of a state agency or his/her designee.

(4) Required receipts for conference expenses

Receipts are required for expenses exceeding ten dollars. Any applicable conference materials such as agendas, brochures or otherwise shall be required as supporting documentation.

(5) Direct payment

Instead of reimbursing a state agent for his/her conference expenses, a state agency may make direct payment to a vendor who provides event services for the state agent.

(H) Agency contractors

State agencies desiring to reimburse travel, lodging, and meal expenses should negotiate such reimbursement with the contractor or vendor when negotiating the cost of the contract, but shall not negotiate rates higher than those authorized by this rule.

(I) Non-reimbursable travel expenses

"Non-reimbursable travel expense" include, but are not limited to, the following:

(1) Alcoholic beverages purchased by the state agent;

(2) Entertainment expenses paid by the state agent;

(3) Incidental expenses, which include personal expenses incurred during travel that are primarily for the benefit of the state agent and not directly related to the official purpose of the travel. Examples include, but are not limited to, the purchase of personal hygiene items, magazines or books, movie rentals, and other miscellaneous items;

(4) Political expenses paid by the state agent;

(5) Travel insurance expenses paid by the state agent; for purposes of this paragraph, the use of the term "travel insurance expense" does not mean liability coverage and loss damage waiver expenses incurred in renting an automobile pursuant to paragraph (C)(3)(d) of this rule.

(6) The cost of traffic fines and parking tickets.

(J) Exceptions may be requested by submitting a written request to the director of budget and management by the head of a state agency or his/her designee prior to the expense being incurred. The director of the office of budget and management may grant exceptions to this rule only for travel by law enforcement officials, insurance examiners, state agents on continuous travel status for two or more consecutive days, state agents requiring special travel arrangements due to a disability, and state agents whose workday is other than eight a.m. to five p.m. or if state agents whose in-state travel and lodging arrangements are economically advantageous to the state. Other exceptions may be granted upon a written request submitted to the director of budget and management by the head of a state agency or his/her designee prior to the expense being incurred or, at the director's discretion, after the expense has been incurred. No exception shall remain in effect for more than one fiscal year.

(K) Amendment to this rule

An amendment to this rule applies to travel on or after the effective date of the amendment.

EXHIBIT 3

STATE OF OHIO
DEPARTMENT OF ADMINISTRATIVE SERVICES

STANDARD AFFIRMATION AND DISCLOSURE FORM
EXECUTIVE ORDER 2019-09D

Banning the Expenditure of Public Funds on Offshore Services

CONTRACTOR/SUBCONTRACTOR AFFIRMATION AND DISCLOSURE:

By the signature affixed to this response, the CONTRACTOR/SUBCONTRACTOR affirms, understands and will abide by the requirements of Executive Order 2019-09D. If awarded a contract, the CONTRACTOR/SUBCONTRACTOR becomes the Contractor and affirms that both the Contractor and any of its subcontractors shall perform no services requested under this Contract outside of the United States.

The CONTRACTOR/SUBCONTRACTOR shall provide all the name(s) and location(s) where services under this Contract will be performed in the spaces provided below or by attachment. Failure to provide this information as part of the response will deem the CONTRACTOR/SUBCONTRACTOR not responsive the contract will not be executed. If the CONTRACTOR/SUBCONTRACTOR 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 stored, accessed, tested, maintained or backed-up, by Contractor:

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

Name/Location(s) where state data will be stored, accessed, tested, maintained or backed-up by subcontractor(s):

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

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

4. Location where services to be performed will be changed or shifted by Contractor:

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

Name/Location(s) where services will be changed or shifted to be performed by subcontractor(s):

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

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

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

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.

Acknowledged by:

_____
Signature

_____
Name (Print)

_____
Title

_____
Date

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.

Acknowledged by:

_____
Signature

_____
Name (Print)

_____
Title

_____
Date

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.