NOTICE

This opportunity is being released to DBITS Contractors pre-qualified as a result of the MBE RFP #0A1139 and the Open Market RFP #0A1147.

ONLY Contractors pre-qualified in Category Three the Applications Development and Maintenance Transition Planning Category are eligible to submit proposal responses AND to submit inquiries. The State does not intend to respond to inquiries or to accept proposals submitted by organizations not pre-qualified in this Technology Category.

An alphabetical listing of Contractors pre-qualified to participate in this opportunity follows:

Accenture	MGT of America, Inc.
Advocate Consulting Group	Navigator Management Partners LLC
Advocate Solutions LLC	Optimum Technology
American Business Solutions	Peerless Technologies
Ardent Technologies	Persistent Systems
CapTech Ventures	Planet Technologies
Cardinal Solutions Group	Prelude System
Careworks Tech	Proteam Solutions, Inc.
CDI Corp	Quantrum LLC
CDO Technologies, Inc.	Quick Solutions
Centric Consulting LLC	R. Dorsey & Company
CGI Technologies and Solutions, Inc.	Sense Corporation
Cluster Software, Inc.	Sogeti USA, LLC
CMA Consulting Services	Sophisticated Systems, Inc.
Computer Aid, Inc.	Sondhi Solutions
Crowe Horwath LLP	Srisys, Inc.
Data Transfer Solutions	Stellar Innovations & Solutions, Inc.
Data-Core Systems, Inc.	Strategic System's Inc.
Digitek Software, Inc.	System Soft Technologies
Diversified Systems, Inc.	Systems Technology Group, Inc.
enfoTech	TCC Software Solutions
Evanhoe & Associates	Team Ray Technologies, LLC
Flairsoft	TEK Systems
Halcyon Solutions, Inc.	Teranomic
HMB, Inc.	The Greentree Group
IBM	TMH Solutions
IIT	Truven Health Analytics

Infojini	Unicon International. Inc.
Information Control Company	Vana Solutions
JMT Technology Group	Ventech Solutions, Inc.
Kunz, Leigh & Associates	Vertex
Lochbridge	Windsor Solutions
Logic Soft, Inc.	XLN Systems
Mapsys Systems & Solutions	
MAXIMUS Human Services, Inc.	
McGladrey LLP	

Statement of Work Solicitation

State of Ohio Ohio Department of Job and Family Services Ohio Job Insurance Password Reset Project Statement of Work	DBITS Solicitation ID No.	Solicitation Release Date
	DBJFS-19-03-001	08-28-2018

Section 1: Purpose

The purpose of this Project Statement of Work (SOW) is to provide Ohio Department of Job and Family Services (ODJFS) with information technology services in Technology Category Application Development and Maintenance Transition Planning. A qualified Contractor, herein after referred to as the "Contractor", shall furnish the necessary personnel, equipment, material and/or services and otherwise do all things necessary for or incidental to the performance of work set forth in Section 3, *Scope of Work*.

Table of Contents

Supplements

Timeline

SOW Solicitation Release to Contractor:	August 28, 2018
Inquiry Period Begins:	August 28, 2018
Inquiry Period Ends:	September 11, 2018 at 8:00 AM
Proposal Response Due Date:	September 18, 2018 at 1:00 PM

Section 2: Background Information

2.1 Agency Information

Agency Name	Ohio Department of Job and Family Services (ODJFS)		
Contact Name	Maureen Ahern-Wantz, Business Relationship Manager	Contact Phone	614-915-2334
Bill to Address	Ohio Department of Job and Family Services (ODJFS)		

	Office of Fiscal and Monitoring Service 30 East Broad St., 37th Floor Columbus, OH 43215

2.2 Project Information

Project Name	Ohio Job Insurance (OJI) Password Reset
Project Background & Objective	The Ohio Job Insurance help desk call center experiences many password reset requests. To improve customer service, ODFJS has determined that implementation of Conversational UI and Robotic Automation Processing can be utilized as a solution. The goal of the project is to implement technology to reduce the need for call center support and get experience with chat and bot technology. This engagement is to implement a solution to automate the current process that the call center staff use to validate that a password reset is being requested by the appropriate entity, confirm preferred interfaces (email or US Mail), then trigger a PIN reset on the OJI system screen. This will result in either an email with an immediate link to reset their PIN or a piece of US mail going out the next day with the PIN. The implementation will include training and knowledge transfer to OIS Staff for the configuration of the software and related implementation as well as ongoing maintenance and monitoring processes. The solution must be Azure cloud based Microsoft BOT Framework and LUIS technology to support this type of Robotic Process Automation. This combination can address these requirements and provide capabilities to address similar automation in other business processes.
Expected Project Duration	Expected duration of this project is three (3) months. The Contractor must present a timeline based on their experience in this type of project and the expected deliverables defined by ODJFS.

2.3 Project Schedule

Date	Task
Second Quarter 2018	Project start
Within 10 days of award	Kickoff meeting to include Detailed Project Plan and Schedule
Within 30 days of award	Configuration completed and system testing in progress
Within 60 days of award	Completion of system test, staff training and production implementation
45 days after production implementation	Provide technical support as needed to resolve performance issues, configuration and process flow issues and resolution support.

2.4 Project Milestones

Date	Milestone
Within 10 days of award	Detailed Project Plan and Schedule
Within 30 days of award	Configuration completed and system testing in progress

Within 60 days of award	Completion of systems testing, staff training and production implementation
45 days after production implementation	Provide technical support as needed to resolve performance issues, configuration and process flow issues and resolution support.

2.5 Contractor's Work Effort Requirement

The Contractor's full-time regular employees must perform at least 30% of the effort required to complete the Work. The Contractor must use its personnel or subcontractor personnel to meet the remaining 70% of the effort. The same Contractor team members for the duration of the project is required.

2.6 Ohio Certified MBE Set-Aside Requirement

- This solicitation is being released as an Open Market and MBE solicitation to pre-qualified MBE Contractors under RFP Contracts 0A1139 and 0A1147.

Section 3: Scope of Work

3.1 ODJFS OJI – Password Reset Requirements

In SCOPE

1. Technology implemented must be MS Bot Framework, LUIS technology
2. Technology must utilize a configuration framework that requires minimal programming or scripting language skills.
3. Collection and documenting the OJI manual reset process requirements and designing the solution and configuration requirements.
4. Configure the solution to intercept phone call from the ODJFS IVR system.
5. Configure the solution to prompt for the required data through numeric entry from the phone keypad.
6. Configure the solution to prompt for the required data using speech recognition.
7. Configure the solution to use the data collected to perform automated data entry to the appropriate OJI screens to process the password request.
8. Configure the solution to enable transfer to the help desk when automated data entry cannot be initiated.
9. Support production implementation for 45 days after acceptance of production implementation.
10. Train staff on configuration and maintenance of the solution.
11. System performance testing to ensure solution meets or exceeds processing time of current password reset process.
12. System stress testing and tuning to ensure processes are performing as expected and provide a positive experience to the OJI customer seeking a password reset.

Out of SCOPE

1. Business processes other than the OJI password reset process.
2. Implementation of Ohio Digital eXperience (ODX) solution for password reset.
3. Evaluating multiple vendor software solutions.
4. Developing custom code using Java, .Net or any other programming language.
5. Modification of the OJI data entry screens or any other systems processes.
6. Purchase of any hardware to include, but not limited to, servers and networking.
7. Cloud based technology not hosted in USA.
8. Software technology that does not have a USA based office and services organization.
9. Performance tuning of the OJI online system to handle Robotic Process Automation.

3.2 Assumptions and Constraints

Assumptions	Software or subscription services will be required and temporary licensing may be required to meet project schedule.
	Contractor or subcontractor will provide resources that have in depth experience in MS Bot framework technology.
	The selected Contractor or subcontractor will provide project management support and is responsible for scheduling all meetings, establishing project approach and coordinating support with ODJFS.
	Travel expenses are the responsibility of the Contractor and will not be billed back to ODJFS.
	Contractor or subcontractor will provide resources that have in depth experience in proposed technology.
	No programming changes to either the OJI system or the IVR system supporting the call center
Constraints	ODJFS may provide hoteling cubical space for up to three (3) staff at 4200 East Fifth Avenue, Columbus, OH 43219.

3.3 Deliverable Descriptions

- Deliverables must be provided on the dates specified. Any changes to the delivery date must have prior approval (in writing) by the ODJFS contract manager or designate.
- All deliverables must be submitted in a format approved by the ODJFS contract manager.
- All deliverables must have acceptance criteria established and a time period for testing or acceptance.
- If the deliverable cannot be provided within the scheduled time frame, the Contractor is required to contact the ODJFS contract manager in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.
- A request for a revised schedule must be reviewed and approved by the ODJFS contract manager before placed in effect.
- ODJFS will complete a review of each submitted deliverable within specified working days of the date of receipt.
- A kickoff meeting will be held at a location and time selected by the ODJFS where the Contractor and its staff will be introduced to the ODJFS.

3.4 Deliverable Name	Deliverable Description
1. Detailed Project Plan and Schedule	Provide a detailed project plan and schedule of activities required for the project. Define the tools and methods for developing the deliverables and related documentation. The project plan must include a plan for change control of any scripts or other provisioned data.
2. Configuration and Systems Testing	Configure and conduct systems testing that includes integration with the IVR and OJI systems security and related online screens that manage password reset. Provide documentation on systems design, systems performance capabilities for transaction processing, steps for problem resolution and related maintenance requirements to ensure system performs as expected.
3. Completion of systems testing, staff training and production implementation	Systems documentation completed and accepted by ODJFS, training and knowledge transfer completed, systems stress testing and performance meet ODJFS requirements, documentation for known work arounds and problem resolution steps, documented migration processes and related change management processes to migrate to production environment, migration to production and system activation.

3.4 Deliverable Name	Deliverable Description
4. Completion of forty-five (45) days of technical support after production implementation of the Robotic Automation OJI password reset solution	Provide on-site and/or remote technical assistance for problem resolution to include assisting with technical changes, debugging processing issues and implementing configuration changes for problem resolution, documentation of defects and actions required for resolution.

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
1. Detailed Project Plan and Project Schedule	10 days after award	No	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor
2. Configuration and Systems Testing	30 days after award	No	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor
3. Completion of systems testing, staff training and production implementation	60 days after award	Yes 80%	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor
4. Completion of forty-five (45) days of technical support after production implementation	45 days after production implementation	Yes 20%	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor

3.5 Roles and Responsibilities

Project or Management Activity/Responsibility Description	Contractor	ODJFS
Project Schedule and Deliverables	X	
Coordinating State contacts, email accounts, work space and related support		X
ODJFS Project Manager to assist with managing State staff, review status reports, assist with project issue resolution and related activities to support the project		X

3.6 Restrictions on Data Location and Work

- The Contractor must perform all Work specified in the SOW Solicitation and keep all State data within the United States, and the State may reject any SOW Response that proposes to do any work or make State data available outside the United States.

3.7 Resource Requirements

- ODJFS will provide hoteling cubicle space at 4200 East Fifth Avenue, Columbus, OH 43219 for up to three (3) contractor staff members.
- ODJFS will provide access to current call center staff to collect information on password reset procedure.
- ODJFS will make limited time available from an OJI SME for system questions and log files.

Section 4: Deliverables Management

4.1 Submission/Format

PM Artifact/Project Work Product	Submission	Format
Project Plan tasks and Gantt chart	Via email and within 10 days of project start date	Microsoft Project compatible format
Progress Reports	Via email	Microsoft Office compatible format
All project documents are to be delivered electronically	Via email and as required	Microsoft Office compatible format

4.2 Reports and Meetings

- The Contractor is required to provide the ODJFS contract manager with weekly written progress reports of this project. These are due to the ODJFS contract manager by the close of business on Friday each week throughout the life of the project.
- The progress reports shall cover all work performed and completed during the week for which the progress report is provided and shall present the work to be performed during the subsequent week.
- The progress report shall identify any problems encountered or still outstanding with an explanation of the cause and resolution of the problem or how the problem will be resolved.
- The Contractor will be responsible for conducting weekly status meetings with the ODJFS contract manager. The meetings will be held on Monday at a time and place so designated by the ODJFS contract manager – unless revised by the ODJFS contract manager. The meetings can be in person or over the phone at the discretion of the ODJFS contract manager.

4.3 Period of Performance

This project is expected to be completed within one hundred and five (105) days. Performance is based on the delivery and acceptance of each deliverable.

4.4 Performance Expectations

This section sets forth the performance specifications for the Service Level Agreements (SLA) to be established between the Contractor and State. Most individual service levels are linked to "Fee at Risk" due to the State to incent Contractor performance.

The Service Levels contained herein are Service Levels this SOW Solicitation. Both the State and the Contractor recognize and agree that Service Levels and performance specifications may be added or adjusted by mutual agreement during the term of the Contract as business, organizational objectives and technological changes permit or require.

The Contractor agrees that 10% of the not to exceed fixed price for the SOW will be at risk ("Fee at Risk"). The Fee at Risk will be calculated as follows:

Total Not to Exceed Fixed Price (NTEFP) of the SOW	x	10 %	=	Total Fee at Risk for the SOW

Furthermore, in order to apply the Fee at Risk, the following monthly calculation will be used:

Monthly Fee At Risk	=	Total Fee at Risk for the SOW Term of the SOW in months

The Contractor will be assessed for each SLA failure and the "Performance Credit" shall not exceed the monthly Fee at Risk for that period. The Performance Credit is the amount due to the State for the failure of SLAs. For SLAs measured on a quarterly basis, the monthly fee at risk applies and is cumulative.

On a quarterly basis, there will be a "true-up" at which time the total amount of the Performance Credit will be calculated (the "Net Amount"), and such Net Amount may be off set against any fees owed by the State to the Contractor, unless the State requests a payment in the amount of the Performance Credit.

The Contractor will not be liable for any failed SLA caused by circumstances beyond its control, and that could not be avoided or mitigated through the exercise of prudence and ordinary care, provided that the Contractor promptly, notifies the State in writing and takes all steps necessary to minimize the effect of such circumstances and resumes its performance of the Services in accordance with the SLAs as soon as reasonably possible.

To further clarify, the Performance Credits available to the State will not constitute the State's exclusive remedy to resolving issues related to the Contractor's performance. In addition, if the Contractor fails multiple service levels during a reporting period or demonstrates a pattern of failing a specific service level throughout the SOW, then the Contractor may be required, at the State's discretion, to implement a State-approved corrective action plan to address the failed performance.

SLAs will commence when the SOW is initiated.

Monthly Service Level Report. On a monthly basis, the Contractor must provide a written report (the "Monthly Service Level Report") to the State which includes the following information:

- Identification and description of each failed SLA caused by circumstances beyond the Contractor's control and that could not be avoided or mitigated through the exercise of prudence and ordinary care during the applicable month;
- the Contractor's quantitative performance for each SLA;
- the amount of any monthly performance credit for each SLA;
- the year-to-date total performance credit balance for each SLA and all the SLAs;
- upon state request, a "Root-Cause Analysis" and corrective action plan with respect to any SLA where the Individual SLA was failed during the preceding month; and
- trend or statistical analysis with respect to each SLA as requested by the State.

The Monthly Service Level Report will be due no later than the tenth (10th) day of the following month.

SLA Name	Performance Evaluated	Non-Conformance Remedy	Frequency of Measurement
Delivery Date Service Level	The **Delivery Date Service Level** will measure the percentage of SOW tasks, activities, deliverables, milestones and events assigned specific completion dates in the applicable SOW and/or SOW project plan that are achieved on time. The State and the Contractor will agree to a project plan at the commencement of the SOW and the Contractor will maintain the project plan as agreed to throughout the life of the SOW. The parties may agree to re-baseline the project	Fee At Risk	Monthly or At the time of estimated deliverable due dates.

	plan throughout the life of the SOW. Due to the overlapping nature of tasks, activities, deliverables, milestones and events a measurement period of one calendar month will be established to serve as the basis for the measurement window. The Contractor will count all tasks, activities, deliverables, milestones and events to be completed during the measurement window and their corresponding delivery dates in the applicable SOW and/or SOW project plan. This service level will commence upon SOW initiation and will prevail until SOW completion. **Compliance with delivery date is expected to be greater than 85%** This SLA is calculated as follows: "% Compliance with delivery dates" equals "(Total dates in period – Total dates missed)" divided by "Total dates in period"		
Deliverable Acceptance Service Level	The **Deliverable Acceptance Service Level** will measure the State's ability to accept Contractor deliverables based on submitted quality and in keeping with defined and approved content and criteria for Contractor deliverables in accordance with the terms of the Contract and the applicable SOW. The Contractor must provide deliverables to the State in keeping with agreed levels of completeness, content quality, content topic coverage and otherwise achieve the agreed purpose of the deliverable between the State and the Contractor in accordance with the Contract and the applicable SOW. Upon mutual agreement, the service level will be calculated / measured in the period due, not in the period submitted. Consideration will be given to deliverables submitted that span multiple measurement periods. The measurement period is a quarter of a year. The first quarterly measurement period will commence on the first day of the first full calendar month of the Contract, and successive quarterly measurement period will run continuously thereafter until the expiration of the applicable SOW. **Compliance with deliverable acceptance is expected to be greater than 85%** . This SLA is calculated as follows: "% Deliverable Acceptance" equals "# Deliverables accepted during period" divided by "# Deliverables submitted for review/acceptance by the State during the period"	Fee At Risk	Monthly or At the time of estimated deliverable due dates.

4.5 State Staffing Plan

Staff/Stakeholder Name	Project Role	Percent Allocated
ODJFS	Project Manager/Contract Manager	10%
ODJFS	Subject matter expert for OJI system and log files	10%
ODJFS	Technology Support	50%

Section 5: SOW Response Submission Requirements

5.1 Response Format, Content Requirements

An identifiable tab sheet must precede each section of a Proposal, and each Proposal must follow the format outlined below. All pages, except pre-printed technical inserts, must be sequentially numbered.

Each Proposal must contain the following:

1. Cover Letter
2. Contractor Experience Requirements
3. Subcontractors Documentation
4. Assumptions
5. Payment Address
6. Staffing plan, personnel resumes, time commitment, organizational chart
7. Contingency Plan
8. Project Plan
9. Project Schedule (WBS using MS Project or compatible)
10. Communication Plan
11. Risk Management Plan
12. Quality Management Plan
13. Fee Structure
14. Acceptance of Security and Privacy Supplement (Supplement 1) and ODJFS-DAS Security Supplement Addendum (Supplement 2)
15. Rate Card

Include the following:

1. Cover Letter:

a. Must be in the form of a standard business letter;

b. Must be signed by an individual authorized to legally bind the Contractor;

c. Must include a statement regarding the Contractor's legal structure (e.g. an Ohio corporation), Federal tax identification number, and principal place of business; please list any Ohio locations or branches;

d. Must include a list of the people who prepared the Proposal, including their titles; and

e. Must include the name, address, e-mail, phone number, and fax number of a contact person who has the authority to answer questions regarding the Proposal.

2. Contractors or subcontractor's Experience Requirements (see Section 6 for additional information required with submission for evaluation)

a. Each proposal must include a brief executive summary of the services the Contractor proposes to provide and one representative sample of previously completed projects as it relates to this proposal (e.g. detailed requirements documents, analysis);

b. Each proposal must describe the Contractor's or subcontractor's experience, capability, and capacity to provide Conversational User Interface and/or Robotic Automation solutions. Provide specific detailed information demonstrating experience similar in nature to the type of work described in this SOW for each of the resources identified in Section 5.2.

c. At least one team member must possess knowledge of MS LUIS Conversational UI and/or MS Bot Framework with production implementation.

d. Project Team Qualifications: Provide an outline of the project team and a brief description on the approach for the project. At a minimum, the proposal must contain Proposed team members resume or curriculum vitae demonstrating that the team has the necessary professional experience and background.

3. Subcontractor Documentation:

a. For each proposed Subcontractor, the Contractor must attach a letter from the subcontractor, signed by someone authorized to legally bind the subcontractor, with the following included in the letter:

1) The Subcontractor's legal status, federal tax identification number, D-U-N-S number if applicable, and principal place of business address;

2) The name, phone number, fax number, email address, and mailing address of a person who is authorized to legally bind the Subcontractor to contractual obligations;

3) A description of the work the Subcontractor will do and one representative sample of previously completed projects as it relates to this SOW (e.g. detailed requirements document, analysis, statement of work);

4) Must describe the Subcontractor's experience, capability, and capacity to provide Application Development and Maintenance Transition Planning. Provide specific detailed information demonstrating experience similar in nature to the type of work described in this SOW from each of the resources identified in Section 5.2;

5) A commitment to do the work if the Contractor is selected; and

6) A statement that the Subcontractor has read and understood the SOW and will comply with the requirements of the Solicitation.

4. Assumptions: The Contractor must list all assumptions the Contractor made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the Contractor remove the assumption or choose to reject the Proposal. No assumptions may be included regarding the outcomes of negotiation, terms and conditions, or requirements. Assumptions should be provided as part of the Contractor response as a stand-alone response section that is inclusive of all assumptions with reference(s) to the section(s) of the RFP that the assumption is applicable to. The Contractor should not include assumptions elsewhere in their response.

5. Payment Address: The Contractor must give the address to which the State should send payments under the Contract.

6. Staffing plan, personnel resumes, time commitment, organizational chart

Identify Contractor and sub-contractor staff and time commitment. Identify hourly rates for personnel, as applicable.

Include Contractor and sub-contractor resumes for each resource identified and organizational chart for entire team.

Contractor Name	Role	Contractor or Sub-contractor?	No. Hours	Hourly Rate

7. Contingency Plan

Identify and provide a contingency plan, should the contractor and/or subcontractor staff fail to meet the Project Schedule, Project Milestones or fail to complete the deliverables according to schedule. Include alternative strategies to be used to ensure project success if specified risk events occur.

8. Project Plan

Identify and describe the plan to produce effective documents and complete the deliverable requirements. Describe the primary tasks, how long each task will take and when each task will be completed to meet the final deadline.

9. Project Schedule (WBS using MS Project or compatible)

Describe the Project Schedule including planning, planned vs. actuals for monitoring performance, milestones, and detailed tasks. Using MS Project create a deliverable-oriented grouping of project elements that organizes and defines the total work scope of the project with each descending level representing an increasingly detailed definition of the project work.

10. Communication Plan

Describe the format and method for weekly updates on project status and escalation procedures that ODJFS will take if contract deliverables are not being met.

11. Risk Management Plan

Describe the Risk Management Plan requirements including the risk factors, associated risks and likelihood of occurrence including consequences for each risk. Describe your plan for mitigating selected risks and plan for keeping people informed about those risks throughout the project.

12. Quality Management Plan

Describe your quality policies, procedures, and standards relevant to the project for both project deliverables and project processes. Define who is responsible for the quality of the delivered project artifacts and deliverables.

13. Fee Structure including Estimated Work Effort for each Deliverable

Payment will be scheduled upon approval and acceptance of each Deliverable by the Contract Manager within the usual payment terms of the State.

Deliverable Name	Total Estimated Work Effort (Hours)	Not-to-Exceed Fixed Price for Deliverable
Detailed Project Plan and Project Schedule		N/A

Deliverable Name	Total Estimated Work Effort (Hours)	Not-to-Exceed Fixed Price for Deliverable
Configuration and Systems Testing		N/A
Completion of systems testing, staff training and production implementation (80% of total)		
Completion of forty-five (45) days of technical support after production implementation (20% of total)		
	Total Not-to-Exceed Fixed Price for all Deliverables	

14. Acceptance of Security and Privacy Supplement (Supplement 1) and JFS-DAS Security Supplement Addendum (Supplement 2)

The Contractor must provide a statement agreeing to and accepting Supplement 1 (Security and Privacy Supplement) and Supplement 2 (ODJFS-DAS Security Supplement Addendum) in their entirety.

15. Rate Card

Describe submission and format requirements for Contractors to submit a Rate Card, as applicable. The primary purpose of obtaining this Rate Card information is to establish baseline hourly rates in the event that change orders are necessary. The DBITS contract is not intended to be used for hourly based time and materials work. (NOTE – Section 5.2 collects rate information for named resources)

Position	Hourly Rate
	$
	$
	$

Section 6: SOW Evaluation Criteria

Mandatory Requirements: Accept/Reject

1. Each proposal must include a brief executive summary of the services the Contractor proposes to provide and one representative sample of previously completed projects as it relates to this proposal (e.g. Robotic Process Automation Implementation);
2. Each proposal must describe the Contractor's or subcontractor's experience, capability, and capacity to provide Conversational User Interface and/or Robotic Automation solutions. Provide specific detailed information demonstrating experience similar in nature to the type of work described in this SOW for each of the resources identified in Section 5.2.
3. At least one team member must possess knowledge of MS LUIS Conversational UI and/or MS Bot Framework with production implementation.
4. Project Team Qualifications: Provide an outline of the project team and a brief description on the approach for the project. At a minimum, the proposal must contain proposed team members resume or curriculum vitae demonstrating that the team has the necessary professional experience and background.

Scored Requirements	Weight	Does Not Meet	Meet	Exceeds
Contractor or subcontractor summary show(s) company experience in implementing Conversational UI and/or robotic automation.	6	0	5	7
Project plan, staffing and timeline proposed demonstrates the ability to complete the project within the desired timeline defined by ODJFS.	4	0	5	7
Contractor demonstrates understanding of the requirements detailed in the SOW and the ability to successfully design, build and deploy a OJI password reset solution.	5	0	5	7

Price Performance Formula. The evaluation team will rate the Proposals that meet the Mandatory Requirements based on the following criteria and respective weights.

Criteria	Percentage
Technical Proposal	70%
Cost Summary	30%

To ensure the scoring ratio is maintained, the State will use the following formulas to adjust the points awarded to each offeror.

The offeror with the highest point total for the Technical Proposal will receive 700 points. The remaining offerors will receive a percentage of the maximum points available based upon the following formula:

Technical Proposal Points = (Offeror's Technical Proposal Points/Highest Number of Technical Proposal Points Obtained) x 700

The offeror with the lowest proposed total cost for evaluation purposes will receive 300 points. The remaining offerors will receive a percentage of the maximum cost points available based upon the following formula:

Cost Summary Points = (Lowest Total Cost for Evaluation Purposes/Offeror's Total Cost for Evaluation Purposes) x 300

Total Points Score: The total points score is calculated using the following formula:

Total Points = Technical Proposal Points + Cost Summary Points

Section 7: SOW Solicitation Calendar of Events

Firm Dates

SOW Solicitation Released to Contractors	August 28, 2018

Inquiry Period Begins	August 28, 2018
Inquiry Period Ends	September 11, 2018
Proposal Response Due Date	September 18, 2018 1:00 pm

Anticipated Dates

Estimated Date for Selection of Awarded Contractor	October 2018
Estimated Commencement Date of Work	October 2018

All times listed are Eastern Standard Time (EST).

SECTION 8: Inquiry Process

Contractors may make inquiries regarding this SOW Solicitation anytime during the inquiry period listed in the Calendar of Events. To make an inquiry, Contractors must use the following process:

- Access the State's Procurement Website at http://procure.ohio.gov/;
- From the Navigation Bar on the left, select "Bid Opportunities Search";
- Select the "Doc/Bid Number" textbox;
- Enter the DBITS Solicitation ID number found on the first page of this SOW Solicitation;
- Click the "Search" button;
- On the Opportunity Search Results page, click on the hyperlinked Bid Number;
- On the Procurement Opportunity Search Detail page, click the "Submit Inquiry" button;
- On the Opportunity Document Inquiry page, complete the required "Personal Information" section by providing:
    - First and last name of the Contractor's representative who is responsible for the inquiry,
    - Name of the Contractor,
    - Representative's business phone number, and
    - Representative's email address;
- Type the inquiry in the space provided including:
    - A reference to the relevant part of this SOW Solicitation,
    - The heading for the provision under question, and
    - The page number of the SOW Solicitation where the provision can be found; and
- Click the "Submit" button.

A Contractor submitting an inquiry will receive an acknowledgement that the State has received the inquiry as well as an email acknowledging receipt. The Pre-Qualified Contractor will not receive a personalized response to the question nor notification when the State has answered the question.

Contractors may view inquiries and responses on the State's Procurement Website by using the "Bid Opportunities Search" feature described above and by clicking the "View Q & A" button on the document information page.

The State usually responds to all inquiries within three (3) business days of receipt, excluding weekends and State holidays. But the State will not respond to any inquiries received after 8:00 a.m. on the inquiry end date.

The State does not consider questions asked during the inquiry period through the inquiry process as exceptions to the terms and conditions of this RFP.

Section 9: Submission Instructions & Location

Each Contractor must submit **five (5)** printed, sealed and signed copies of its Proposal Response and each submission must be clearly marked **" OJI Password Reset – DBJFS-19-03-001"** on the outside of its package along with Contractor's name.

A single electronic copy of the complete Proposal Response in PDF format must also be submitted with the printed Proposal Responses. Electronic submissions should be on a CD, DVD or USB memory stick.

Each proposal must be organized in the same format as described in Section 5. Any material deviation from the format outlined in Section 5 may result in a rejection of the non-conforming proposal. Each proposal must contain an identifiable tab sheet preceding each section of the proposal. Proposal Response should be good for a minimum of 60 days.

The State will not be liable for any costs incurred by any Contractor in responding to this SOW Solicitation, even if the State does not award a contract through this process. The State may decide not to award a contract at the State's discretion. The State may reject late submissions regardless of the cause for the delay. The State may also reject any submissions that it believes is not in its interest to accept and may decide not to do business with any of the Contractors responding to this SOW Solicitation.

Proposals are due no later than the date and time specified in Section 7 Solicitation Calendar of Events. No responses will be accepted after this date and time. Proposal Responses MUST be submitted to the State Agency's Procurement Representative:

Ohio Department of Job and Family Services
Office of Contracts and Acquisitions
OJI Password Reset Automation
Attention: Jay Easterling
30 E. Broad St., 31st Floor
Columbus, OH 43215

Proprietary information

All Proposal Responses and other material submitted will become the property of the State and may be returned only at the State's option. Proprietary information should not be included in a Proposal Response or supporting materials because the State will have the right to use any materials or ideas submitted in any quotation without compensation to the Contractor. Additionally, all Proposal Response submissions will be open to the public after the contract has been awarded.

The State may reject any Proposal if the Contractor takes exception to the terms and conditions of the Contract.

Waiver of Defects

The State has the right to waive any defects in any quotation or in the submission process followed by a Contractor. But the State will only do so if it believes that is in the State's interest and will not cause any material unfairness to other Contractors.

Rejection of Submissions

The State may reject any submissions that is not in the required format, does not address all the requirements of this SOW Solicitation, or that the State believes is excessive in price or otherwise not in its interest to consider or to accept. The State will reject any responses from companies not in the Technology Category associated with this SOW Solicitation. In addition, the State may cancel this SOW Solicitation, reject all the submissions, and seek to do the work through a new SOW Solicitation or other means.

Section 10: Limitation of Liability

Unless otherwise stated in this section of the SOW Solicitation, the Limitation of Liability will be as described in Attachment Four, Part Four of the Contract General Terms and Conditions.

Supplement 1

Supplement 1: Current Procedure: OJI Manual Password Reset

Current Procedure: OJI Manual Password Reset

1) Call comes in to designated staff supporting password reset telephone option line
2) Staff confirms the identity of the person calling (they check 5 items) such as:
    a. Asks name
    b. Asks SSN
    c. Asks address
    d. Date of birth
    e. Email address
    f. identification number (dl or state id)
    g. phone number
3) Confirms correspondence preference – US mail vs email
    a. If US Mail – tries to convince them to provide an email address (emails received within 1 minute, mail received within 5 days)
    b. If email
        i. If new email address is provided; add to account and verify
        ii. If continuous email address verifies the one we have is accurate
    c. Save any changes made
    d. Select “pin History”
    e. Select “send new pin”
    f. Verify
        i. Successful new pin generated
        ii. If errors, or pin did not generate make corrections and select “send new pin”
    g. Verify claimant receives pin received (and is able to successfully log in before hanging up if time permits)

Supplement 2

State IT Computing Policy Requirements

State Architecture and Computing Standards Requirements

State Security and Privacy Requirements

State Data Handling Requirements

Version Identifier:	Date:
2.0	8/29/2016
3.0	9/27/2016
4.0	1/10/2017
5.0	1/31/2017

Contents

• Overview and Scope

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 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; and
- 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 additive to the Standard State Terms and Conditions contained elsewhere in this contract. In the event of a conflict for whatever reason, the highest standard contained in this contract shall prevail.

• State IT Policy 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.

State of Ohio IT Policies and Standards

Item	Link
IT Policies and Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx
Statewide IT Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Statewide IT Bulletins	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx
DAS Policies	100-11 Protecting Privacy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series http://das.ohio.gov/Divisions/DirectorsOffice/EmployeesServices/DASPolicies/tabid/463/Default.aspx

• State Architecture and Computing Standards Requirements

1.1. Requirements Overview

Offerors responding to State issued RFQ/RFP requests, and as Contractors performing the work following an award, are required to propose solutions that comply with the standards outlined in this document. In the event Offeror finds it necessary to deviate from any of the standards, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

1.1.1. State of Ohio Standards

The State has a published Core Technology Stack as well as Enterprise Design Standards as outlined in this document and, due to State preferences, each are subject to improvements, elaboration and replacement. The State also provides numerous IT Services in both the Infrastructure and Application categories, as outlined in the State's IT Services Catalog at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

1.1.2. Offeror Responsibilities

Offerors can propose on-premise or cloud-based solutions. When proposing on-premise solutions, Offerors and Contractors must comply with State requirements including using the State's Virtualized Compute Platform. Offerors proposing on-premise solutions are required to install third party applications on State- provided compute platforms. Dedicated server platforms are not compliant with the State's Virtualization Requirements.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, (i.e., Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence). When dedicated Application components (i.e., Application Servers, Databases, etc.) are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards. In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

1.2. Compute Requirements: Client Computing

Offerors **must not** propose solutions that require custom PC's, Laptops, Notebooks etc. The State will source its own Client computing hardware and the Offeror's proposed solutions are required to be compatible with the State's hardware.

1.2.1. Compute Requirements: Server / OS

Offerors **must** propose solutions that comply with the State's supported Server / OS versions.

The following are the State's Required Server and OS versions.

Table 1 – Supported Server/OS versions

Operating Systen	Version	Edition
Microsoft Windows Server	2012, 2012 R2	Standard, Enterprise, & Datacenter
RedHat Linux	7	Enterprise
IBM AIX	7.1	
Oracle Enterprise Linux		Enterprise

When Offerors are proposing on-premise solutions, these solutions must comply with the State's supported Server Compute Platforms.

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State 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 Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

For Ohio Benefits and the Ohio Administrative Knowledge System (OAKS) – Exalogic Version 2.0.6.0.2

1.2.2. Ohio Cloud: Hypervisor Environment

When Offerors are proposing on-premise solutions, these solutions *must* comply with the State's supported VMware vSphere, and IBM Power Hypervisor environment.

For Ohio Benefits and OAKS – Oracle Virtual Manager Version 3.3.1, Xen

1.3. Storage and Backup Requirements

1.3.1. Storage Pools

The State provides three 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.

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Storage Service Offerings.

For Ohio Benefits and OAKS - HA (High Availability) storage used with Mirror configuration.

The pools and their standard use cases are below:
Table 2 – State Supported Storage Pools

Storage Pool	Availability	Performance	Typical Applications
Performance	Highest	Fast	Performance pool suited for high availability applications, with high I/O (databases).
General	High	Fast	General pool suitable for file servers, etc.
Capacity	High	Average	Capacity pool suitable for file servers, images and backup / archive). Not suited for high random I/O.

1.3.2. Backup

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Backup Service Offering.

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

For Ohio Benefits - Symantec NetBackup is the Enterprise backup solution.

1.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)

Offerors **must** propose solutions that work within the State's LAN / WAN infrastructure.

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 and local government.

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

The State provides a high bandwidth internal network for internal applications to communicate across the State's LAN / WAN infrastructure. Normal traffic patterns at major sites should be supported.

Today, the State's WAN (OARnet) consists of more than 1,850 miles of fiber-optic backbone, with more than 1,500 miles of it operating at ultrafast 100 Gbps speeds. The network blankets the state, providing connectivity to all State Government Agencies.

The State of Ohio Network infrastructure utilizes private addressing, reverse proxy technology and Network Address Translation (NAT). All applications that are to be deployed within the infrastructure must be tolerant of these technologies for both internal product interaction as well as external user access to the proposed system, infrastructure or application.

The State network team will review applications requirements involving excessive bandwidth (i.e. voice, video, telemetry, or applications) deployed at remote sites.

1.5. Application Requirements

1.5.1. Application Platforms

When Offerors are proposing on-premise solutions, these solutions *must* be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.)

1.5.2. Open API's

Proposed vendor applications must be developed with standards-based Open API's. An open API is an application program interface that provides programmatic access to software applications. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

1.5.3. SOA (Service Oriented Architecture)

When Offerors are proposing on-premise solutions, these solutions *must* be developed using a standards-based Service Oriented Architecture (SOA) model.

1.6. Database Platforms

Proposed vendor application designs must run on databases that comply with the State's supported Database Platforms.

- IBM DB2 Version 10
- Microsoft SQL Server 2012 or higher
- ORACLE 11G and 12C

1.7. Enterprise Application Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

At a minimum, proposed vendor application designs that include the following Application Services *must* use the Application IT Services outlined in the IT Services Catalog.

1.7.1. Health and Human Services: Integrated Eligibility

The Integrated Eligibility Enterprise platform provides four key distinct technology domains / capabilities:

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

1.7.2. The Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time-and money-saving online filing and payment system that helps simplify business' relationship with Government agencies.

- New Business Establishment – Provides a single, portal based web location for the establishment of new businesses in Ohio, file with the required State agencies and ensure that business compliance requirements of the State are met.
- Single Point Revenue and Fee Collection - Manage payments to State's payment processor (CBOSS) and broker payment to multiple agencies while creating transaction logs and Business Customer "receipts".
- Business One-Stop Filing and Forms - Provides guides and forms to Business Users through complex transactions that have multiple steps, forms and / or filing requirements for users on procedures to complete the process including Agencies and (if applicable) systems they will need to interact with.
- Scheduling and Reminders - Notify Business Customers of a particular event that is upcoming or past due (Filing due) using a "calendar" or "task list" metaphor.
- Collections and Confirmations – Provides a Payment Card Industry (PCI) certified web-based payment solution that supports a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, and cash payments.

1.7.3. Ohio Administrative Knowledge System (OAKS)

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 via myOhio.gov, Enterprise Learning Management, and Customer Relationship Management. Core System Capabilities include (but are not limited to):

Content Management (myohio.gov)

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids, and news
- Statewide Top Stories
- Portal to OAKS applications
- Employee and Contractor Management

Enterprise Business Intelligence

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

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eBid
- eCatalog (Ohio Marketplace)
- eInvoicing
- eSupplier/Offeror Maintenance
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

Customer Relationship Management (CRM)

- Contact / Call Center Management

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery

Human Capital Management (HCM)

- Benefits Administration
- Payroll
- Position Management
- Time and Labor
- Workforce Administration: Employee and Contingent Workers
- Employee Self-Service
- eBenefits
- ePerformance
- Payroll

1.7.4. Enterprise Business Intelligence

- Health and Human Services Information
    - Eligibility
        - Operational Metrics
        - County Caseworker Workload
    - Claims
    - Long Term Care
- Financial Information
    - General Ledger (Spend, Disbursement, Actual/Forecast)
    - Travel and Expense
    - Procure to Pay (AP/PO/Offeror/Spend)
    - Capital Improvements
    - Accounts Receivable
    - Asset Management
- Workforce and Human Resources
    - Workforce Profile
    - Compensation
    - MBE/EDGE

1.7.5. SharePoint

Microsoft SharePoint Server 2013 portal setup and hosting services for agencies interested in internal collaboration, external collaboration, organizational portals, business process workflow, and business intelligence. The service is designed to provision, operate and maintain the State's enterprise Active Directory Accounts.

1.7.6. IT Service Management

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. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.

1.7.7. Enterprise Geocoding Services

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

1.7.8. GIS Hosting

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. User agencies can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications.

1.8. Productivity, Administrative and Communication Requirements

1.8.1. Communication Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

At a minimum, proposed vendor application designs that include the following Communication Services **must** use the Communication Services outlined in the IT Services Catalog.

Exchange

- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing
- External Mail Encryption
- Outbound Fax
- Mobile devices

EDI/Application Integration/Medicaid EDI

Lyris Listserv

On-premise application based FAX

eFAX

- Fax2Mail is a “hosted” fax solution that allows agencies to seamlessly integrate inbound and outbound Fax with their existing desktop E-mail and back-office environments. Fax2Mail is a “cloud-based” solution.

Voice over Internet Protocol (VoIP)

Audio Conference

Video Conference

Call Centers

- ## General State Security and Information Privacy Standards and Requirements

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. The Contractor will implement an information security policy and security capability as set forth in this Contract. The Contractor shall provide the State with contact information for a single point of contact for security incidents.

The Contractor's responsibilities with respect to Security Services will include the following:

- 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 shall provide vulnerability scan results to the State monthly.
- Support the implementation and compliance monitoring for State IT Security Policies.
- Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Manage and administer access to the systems, networks, System software, systems files and State Data, excluding end-users.
- Provide support in implementation of programs to educate State and Contractor end-users and staff on security policies and compliance.
- Install and update Systems software security, assign and reset passwords per established procedures, provide the State access to create User ID's, suspend and delete inactive logon 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, and provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.
- Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Prepare an Information Security Controls Document. This document is the security document that is used to capture the security policies and technical controls that the Contractor will implement, as requested by the State, on Contractor managed systems, supported servers and the LAN within the scope of this contract. The Contractor will submit a draft Information Security Controls document for State review and approval during the transition period.

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide the contractor with contact information for security and program personnel for incident reporting purposes.
- Provide a State Single Point of Contact with responsibility for account security audits.
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies.
- Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.

- Provide the State security 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.
- Assist the Contractor in performing a baseline inventory of access IDs for the systems for which the Contractor has security responsibility.
- Authorize User IDs and passwords for the State personnel for the Systems software, software tools and network infrastructure systems and devices under Contractor management.

1.9. State Provided Elements: Contractor Responsibility Considerations

The State is responsible for Network Layer (meaning the internet Protocol suite and the open systems interconnection model of computer networking protocols and methods to process communications across the IP network) system services and functions that build upon State infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

To the extent that Contractor's accesses or utilizes State- provided networks, the Contractor is responsible for adhering to State policies and use procedures and doing so in a manner that does not diminish established State capabilities and standards.

The Contractor will be responsible for maintaining the security of information in environment elements that it accesses, utilizes, develops or manages in accordance with the State Security Policy. The Contractor will implement information security policies and capabilities, upon review and contract by the State, based on the Contractors standard service center security processes that satisfy the State's requirements contained herein.

The Contractor's responsibilities with respect to Security Services must also include the following:

- Support intrusion detection & prevention, including prompt agency notification of such events, reporting, monitoring and assessing security events. Notification is to be provided to the State for suspected as well as verified security events. For suspected events, the Contractor shall provide regular updates to the State on the status of efforts to verify the event as an actual security event.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software or System Software, [including programs, device drivers, microcode and related code supporting documentation and media] that: 1) perform tasks basic to the functioning of data processing and network connectivity; and 2) are required to operate Applications Software), systems files and the State Data.
- Supporting the State in implementation of programs to raise the awareness of End Users and staff personnel to security risks and to the existence and importance of security policy compliance.
- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user

ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting in processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.

- Developing, implementing, and maintaining a set of automated and manual processes so that the State Data access rules, as they are made known by the State, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under Contractor control.

1.10. Periodic Security and Privacy Audits

The State shall be responsible for conducting periodic security and privacy audits, and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an 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. Dependent on the nature of the issue, the State may elect to contract 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. 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 shall comply with State security and privacy policies.

1.10.1. State Penetration and Controls Testing

The state may, at its sole discretion, elect to perform a Security and Data Protection Audit, at any time, that 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 as to demonstrate that all security, privacy and encryption requirements are met.

State Acceptance Testing will not proceed until the contractor cures all findings, gaps, errors or omissions pertaining to the audit to the state's written satisfaction. Such testing will be scheduled with the contractor at a mutually convenient time during the development and finalization of the project plan, as required by the state.

1.11. Annual Security Plan: State and Contractor Obligations

The Contractor will develop, implement and thereafter maintain annually a Security Plan, that is in alignment with the National Institute of Standards and Technology ("NIST") Special Publication (SP) 800-53 (current, published version), for review, comment and approval by the State Information Security and Privacy Officers. As a minimum, the Security Plan must include and implement processes for the following items related to the system and services:

- Security policies

- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
- Network segmentation
- Perimeter security
- Application security and data sensitivity classification
- PHI and PII data elements
- Intrusion management
- Monitoring and reporting
- Host hardening
- Remote access
- Encryption
- State-wide active directory services for authentication
- Interface security
- Security test procedures
- Managing network security devices
- Security patch management
- Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
- Secure communications over the Internet

The Security Plan must detail how security will be controlled during the implementation of the System and Services and contain the following:

- High-level description of the program and projects
- Security risks and concerns
- Security roles and responsibilities
- Program and project security policies and guidelines
- Security-specific project deliverables and processes
- Security team review and approval process
- Security-Identity management and Access Control for Contractor and State joiners, movers, and leavers
- Data Protection Plan for personal/sensitive data within the projects
- Business continuity and disaster recovery plan for the projects
- Infrastructure architecture and security processes
- Application security and industry best practices for the projects
- Vulnerability and threat management plan (cyber security)

1.12. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including the secure sockets layer (SSL) protocol and public key authentication, signing and 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 PKI. Multi-factor authentication is to be employed for users with privileged network access by leveraging the State of Ohio RSA or Duo Security solutions.

1.13. Security and Data Protection.

All Services must also operate at the [moderate level baseline] as defined in NIST (SP) 800-53 (current, published version) [moderate baseline requirements], be consistent with Federal Information Security Management Act ("FISMA") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Services 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 SLAs and promised operational parameters.

1.14. State Information Technology Policies

The Contractor is responsible for maintaining the security of information in environment elements under direct management of the Contractor and in accordance with State Security policies and standards. The Contractor will implement information security policies and capabilities as set forth in Statements of Work and, upon review and contract by the State, based on the Offeror's standard service center security processes that satisfy the State's requirements contained herein. The Offeror's responsibilities with respect to security services include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Support State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID's, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, providing incident investigation support with the agency's assistance, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State Data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
    - If a security or privacy issue is determined to be pre-existing to this Contract, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract 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.

- 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 is to notify the State within two (2) hours. This notification shall 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 shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract 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.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

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 Section 2, State IT Policy Requirements.

- **State and Federal Data Privacy Requirements**

Because the privacy of individuals' personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public's trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable information in the system is "protected health information" under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not "protected health information" under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

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

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945,45 CFR164.502 (e) and 164.504 (e);
- Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; and
- Corresponding Ohio Administrative Code Rules and Updates.
- 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).
- IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

1.15. Protection of State Data

- **Protection of State Data**. "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, PII and SSI. To protect State Data as described in this Contract, in addition to its other duties regarding State Data, Contractor will: Maintain in confidence any personally identifiable information ("PI")

and State Sensitive Information ("SSI") it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Contract;

- Use and permit its employees, officers, agents, and independent contractors to use any PII/SSI received from the State solely for those purposes expressly contemplated by the Contract;
- Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PII/SSI to any third party, except as permitted under this Contract or required by applicable law, regulation, or court order;
- Take all commercially reasonable steps to (a) protect the confidentiality of PII/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PII/SSI received by the Contractor from the State;
- Give access to PII/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this Contract;
- Upon request by the State, promptly destroy or return to the State in a format designated by the State all PII/SSI received from the State;
- Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
- Establish and maintain data security policies and procedures designed to ensure the following:
  - Security and confidentiality of PII/SSI;
  - Protection against anticipated threats or hazards to the security or integrity of PII/SSI; and
  - Protection against the unauthorized access to, disclosure of or use of PII/SSI.

1.15.1. Disclosure

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

- 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 PII/SSI 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 will promptly notify the State in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will 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 will 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 will use commercially reasonable efforts to obtain confidential treatment for the information;
- To State auditors or regulators;
- 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; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

1.16. Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect State Date from unauthorized disclosure, modification, use or destruction. To accomplish this, the Contractor must adhere to the following principles:

- Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
- Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data.
- 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.
- Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
- Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- Implement and manage security audit logging on information systems, including computers and network devices.

1.17. Contractor Access to State Networks Systems and Data

The Contractor must maintain a robust boundary security capacity 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 points, and disable all others.

To do this, the Contractor must:

- 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.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable information.
- Assume all State Data is both confidential and critical for State operations. The Contractor's security policies, plans, and procedure 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.
- 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.
- 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 appropriate to the situation and may include secure overwriting, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.

- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response 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 with compromised administrator credentials (e.g., keeping periodic copies offline, or in write-only format).

  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 State's 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.
- Not allow the 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 the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas. In addition, all state data on portable media shall be encrypted.
- Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, the State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

1.18. Portable Devices, Data Transfer and Media

Any encryption requirement identified in this Supplement means encryption that complies with National Institute of Standards Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number. Any sensitive State Data transmitted over a network, or taken off site via removable media must be encrypted pursuant to the State's Data encryption standard ITS-SEC-01 Data Encryption and Cryptography.

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 quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

To the extent the State requires the Contractor to adhere to specific processes or procedures in addition to those set forth above in order for the Contractor to comply with the managed services principles enumerated herein, those processes or procedures are set forth in this contract.

1.19. Limited Use; Survival of Obligations.

Contractor may use PII/SSI only as expressly authorized by the Contract and for no other purpose. Contractor's limited right to use PII/SSI expires upon conclusion, non-renewal or termination of this Agreement for any reason. Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

1.20. Disposal of PII/SSI.

Upon expiration of Contractor's limited right to use PII/SSI, Contractor must return all physical embodiments to the State or, with the State's permission; Contractor may destroy PII/SSI. Upon the State's request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PII/SSI in Contractor's possession.

1.21. Remedies

If Contractor or any of its representatives or agents breaches the covenants set forth in these provisions, irreparable injury may result to the State or third parties entrusting PII/SSI to the State. Therefore, the State's remedies at law may be inadequate and the State shall be entitled to seek an injunction to restrain any continuing breach. Notwithstanding any limitation on Contractor's liability, the State shall further be entitled to any other rights or remedies that it may have in law or in equity.

1.22. Prohibition on Off-Shore and Unapproved Access

The Contractor shall comply in all respects with U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export Administration Act ("EAA"); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPAA Privacy Rules and other conventions as described and required in this Supplement.

The Contractor will provide resources for the work described herein with natural persons who are lawful permanent residents as defined in 8 U.S.C. 1101 (a)(20) or who are protected individuals as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state, local), entity.

The State specifically prohibits sending, taking or making available remotely (directly or indirectly) any State information including State Data, software, code, intellectual property, designs and specifications, system logs, system data, personal or identifying information and related materials out of the United States in any manner, except by mere travel outside of the U.S. by a person whose personal knowledge includes technical data; or transferring registration, control, or ownership to a foreign person, whether in the U.S. or abroad, or disclosing (including oral or visual disclosure) or transferring in the United States any State article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or disclosing (including oral or visual disclosure) or transferring data to a foreign person, whether in the U.S. or abroad.

The Contractor shall not use State data for any engagements outside of the scope of the contracted agreement. Using State of Ohio data to test or provide proof-of-concept for other engagements is expressly prohibited.

It is the responsibility of all individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential employee or citizen data associated with Human Resources data, the Contractor will comply with data handling privacy requirements associated with HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in http://www.hhs.gov/ocr/privacysummary.pdf

It is the responsibility of all Contractor individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential or sensitive State, employee, citizen or Ohio Business data associated with State Data, the Contractor will comply with data handling privacy requirements associated with the data HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in http://www.hhs.gov/ocr/privacysummary.pdf.

1.23. Background Check of Contractor Personnel

Contractor agrees that (1) it will conduct 3rd party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Contract. “Ineligible Personnel” means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or 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 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 (“Sensitive Services”).

Upon request, Contractor will provide written evidence that all of Contractor’s personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that 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.

1.24. Federal Tax Information

Contract Language for General Services

1.24.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by its employees with the following requirements:

- All work will be done under the supervision of the Contractor or the Contractor's employees.
- Any 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 will be prohibited.

- All 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.
- The Contractor certifies that the 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 disclosures.
- Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency 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 agency or its designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- All computer systems receiving, processing, storing, or transmitting Federal Tax Information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
- 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 the Contractor fails to provide the safeguards described above.

1.24.2. Criminal/Civil Sanctions

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 IRCs7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
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.

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.

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with Contract safeguards.

- **Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues**

1.25. 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:

- notify the State of the issue or acknowledge receipt of the issue within two (2) hours;
- within forty-eight (48) hours from the initial detection or communication of the issue from the State, present an 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;
- 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 security or privacy until such time as the issue is resolved; and
- upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost.

1.26. 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 PII/SSI by 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:

- Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized Disclosure or Intrusion;
- Investigate and determine if an Intrusion and/or Disclosure has occurred;

- Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion's effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
- Specify corrective action to be taken; and
- Take corrective action to prevent further Disclosure and/or Intrusion.

1.27. Unapproved Disclosures and Intrusions: Contractor Responsibilities

- The Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PII/SSI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.
- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent of an Agency level security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- 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 is to notify the State within two (2) hour. This notification shall 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 shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract 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.

1.28. Security Breach Reporting and Indemnification Requirements

- In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within two (2) hours of the Contractor becoming aware of the breach. In the case of a suspected breach, the Contractor must notify the State in writing of the suspected breach within twenty-four (24) hours of the Contractor becoming aware of the suspected breach.
- The Contractor must fully cooperate with the State to mitigate the consequences of such a breach/suspected breach. This includes any use or disclosure of the State 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.
- 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. The Contractor must document all such incidents/suspected incidents, including its response to them, and make that documentation available to the State on request.
- 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 personally identifiable information is compromised while it is in the Contractor's possession. 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 individuals' credit history through those services.

- **Security Review Services**

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

1.29. 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 should include:

- Deviations to hardware baseline
- Inventory of information types by hardware device
- Software inventory against licenses (State purchased)
- Software versions and then scans of versions against patches distributed and applied

1.30. Security Standards by Device and Access Type

The Contractor will:

- Document security standards by device type and execute regular scans against these standards to produce exception reports
- Document and implement a process for deviation from State standards

1.31. Boundary Defenses

The Contractor will:

- Work with the State to support the denial of communications to/from known malicious IP addresses*
- Ensure that the System network architecture separates internal systems from DMZ and extranet systems
- Require remote login access to use two-factor authentication
- Support the State's monitoring and management of devices remotely logging into internal network
- Support the State in the configuration firewall session tracking mechanisms for addresses that access System

1.32. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Ensure that all systems and environments have adequate space to store logs
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Provide requirements to the State to configure operating systems to log access control events
- Design and execute bi-weekly reports to identify anomalies in system logs

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

1.33. Application Software Security

The Contractor will:

- Perform configuration review of operating system, application and database settings
- Ensure software development personnel receive training in writing secure code

1.34. System Administrator Access

The Contractor will

- Inventory all administrative passwords (application, database and operating system level)
- Implement policies to change default passwords in accordance with State policies, particular following any transfer or termination of personnel (State, existing MSV or Contractor)
- Configure administrative accounts to require regular password changes
- Ensure service level accounts have cryptographically strong passwords
- Store passwords in a hashed or encrypted format
- Ensure administrative accounts are used only for administrative activities
- Implement focused auditing of administrative privileged functions
- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

1.35. Account Access Privileges

The Contractor will:

- Review and disable accounts not associated with a business process
- Create daily report that includes locked out accounts, disabled accounts, etc.
- Implement process for revoking system access
- Automatically log off users after a standard period of inactivity
- Monitor account usage to determine dormant accounts
- Monitor access attempts to deactivated accounts through audit logging
- Profile typical account usage and implement or maintain profiles to ensure that Security profiles are implemented correctly and consistently

1.36. Additional Controls and Responsibilities

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

- Review, Update and Conduct Security training for personnel, based on roles
- Review the adequacy of physical and environmental controls
- Verify the encryption of sensitive data in transit
- Review access control to information based on established roles and access profiles
- Update and review system administration documentation
- Update and review system maintenance policies
- Update and Review system and integrity policies
- Revised and Implement updates to the System security program plan
- Update and Implement Risk Assessment Policies and procedures

- Update and implement incident response procedures

Supplement 3

Supplement 3: JFS-DAS Security Supplement Addendum, revision 1.1

JFS-DAS Security Supplement Addendum

Identity Access Management

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

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

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

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

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

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

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

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

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

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

- Enabling better, more secure access to an ever-growing set of digital services and self-help features across the state through a single proofed identity

- Enabling the state as an organization to consolidate historical transactions and cross-program / agency data to lead a better user experience

An internal ODX Portal acts as the platform by which portal services are provided to agencies. The service portfolio includes:

- Design
- Personalization
- Multitenant and Enterprise Hosting
- Portal and Application Cloud Deployment Control
- Portal Framework
- Integration
- Content Management
- Portlet and Service Consumption and Publishing

Required Interfaces with ODX (where authentication and authorizations are required for applications or services):

Federated Single Sign-on: Application must support federated single sign-on using SAML 2.0 Tokens for identity assertion to authenticate the user to the Application.

Authorization-Based Assertion Attributes: Application, optionally but preferred, would support SAML 2.0 Token assertions to determine appropriate authorizations (roles/permissions) for the individual, upon sign-in, based upon supplied SAML attribute(s) (such as group memberships).

Automation of Provisioning / de-provisioning: Application must support either:

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

Provisioning Tasks that must be available:

- Create, or associate, an identity in the application for authentication and single sign-on.
- Assign and Change an identity's assignment to specific Roles/Permissions within the application for authorization.

De-provisioning Tasks that must be available:

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

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

Encryption

Personally identifiable information (PII), or confidential personal information (CPI - as defined in Ohio Revised Code 1347.15), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. One of the key security controls to protecting PII/CPI is Encryption. Encryption is to be utilized for PII/CPI data on all three states of existence:

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

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

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

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

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

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

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

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

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

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

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

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

- Implement Memory protections, at a minimum, of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) within Hardware and/or Software.
- Sessions must be unique to each authenticated user, and be protected in way that meets the Open Web Application Security Project (OWASP)'s Application Security Verification Standard (ASVS).
- Application will use per user or session indirect object references where possible. All direct object References, from an untrusted source, must include an access control check to ensure the user is authorized for the requested object.

- Ensure that authentication /authorization checks are performed at each object at the controller and business logic levels, and not just at the presentation layer.
- Prevent Injection attacks by using a parameterized API or escape special characters using the specific escape syntax for that interpreter. Also in addition, positive or “white list” input validation must be used.
- Device configurations must confirm to industry best practices for hardening (CIS Benchmarks).
- Components, such as libraries, frameworks, or other software modules used in development must be identified and a list provided to ODJFS at the conclusion of the project. A supported version of these components must be used at time of the contract.
- Autocomplete must be disabled on forms collecting PII/CPI, and caching must be disabled for pages that contain PII/CPI.
- Avoid the use of redirects and forwards as much as possible. When used, any such destination parameters must be a mapped value, and that server side code translates this mapping to the target URL.

Audit Logging

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

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

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

Logging Requirements

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

Required Audit Events:

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

Minimum Logging Requirements for Each Event

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

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

Audit Record Generation Services

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

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

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

Audit Retention, Aggregation, and Analysis

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

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

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