NOTICE

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

ONLY Contractors pre-qualified in Category One the Information Technology Assessment, Planning and Solicitation Assistance Technology 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	Kunz, Leigh & Associates
Advocate Consulting Group	Lochbridge
Advocate Solutions LLC	MAXIMUS Human Services, Inc.
American Business Solutions	Menya Communications, Ltd.
Ardent Technologies Inc.	Optimum Technology
Avasant LLC	McGladrey LLP
Berry Dunn	Menya Communications
CapTech Ventures	MGT of America, Inc.
Cardinal Solutions Group	Navigator Management Partners LLC
Centric Consulting LLC	Peerless Technologies
Cluster Software, Inc.	Proteam Solutions, Inc.
CMA Consulting Services	Persistent Systems
Computer Aid, Inc.	Quantrum LLC
Crowe Horwath LLP	R. Dorsey & Company
CSG Government Solutions	Sense Corp
Evanhoe & Associates	Srisys, Inc.

First Data	Stellar Innovations & Solutions, Inc.
Flairsoft	Sogeti USA, LLC
Gartner	TMH Solutions
Halcyon solutions, Inc.	Sondhi Solutions
HMB, Inc.	Unicon International, Inc.
IBM	System Soft Technologies
IIT Contacts	The Greentree Group
Infojini	UMT Consulting
Information Control Company	Unicon International. Inc.
Information Services Group, Inc.	Vertex
Logic Soft, Inc.	Wild Goose Enterprises, Inc.

Statement of Work Solicitation

State of Ohio Ohio Department of Job and Family Services Software Engineering Strategy System Validation and Continuous Testing	DBITS Solicitation ID No.	Solicitation Release Date
	DBJFS-18-01-008	06-27-2018

Section 1: Purpose

The purpose of this Project Statement of Work (SOW) is to provide the Ohio Department of Job and Family Services (ODJFS) with information technology services in Technology Category Information Technology Assessment, Planning and Solicitation Assistance 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

Timeline

SOW Solicitation Release to Pre-Qualified Contractor:	June 27, 2018
Inquiry Period Begins:	June 27, 2018
Inquiry Period Ends:	July 11, 2018
Proposal Response Due Date:	July 18, 2018 by 1:00 p.m.

Section 2: Background Information

2.2 Project Information

Project Name	Software Engineering Strategy for System Validation and Continuous Testing
Project Background & Objective	ODJFS is in the process of restructuring the technology strategy within the Office of Information Technology (OIS). This project is to review the current Software Engineering processes (requirements, and system test) and provide recommendations for new processes for system validation and continuous testing, that support/plug into DevOps and Agile methodologies. This will include assistance in planning for the modern technologies that are not currently in ODJFS's portfolio.

	This project is to modernize how software is tested and delivered to customers. The recommendations for new processes will ultimately result in quicker delivery to ODJFS's customers.
Expected Project Duration	The estimated duration of this effort will three (3) months. The proposed schedule outlined below is approximate and the pre-qualified Contractor may provide, in their proposal, a more refined estimate and deliverable model, based on this type of work. The estimated start date for this project is August 2018.

2.3 Project Schedule

Date	**Task**
Within 10 days of Award	Kickoff Meeting
Within 15 days of Award	Begin conducting assessment of the current Software Engineering Testing and Validation Process and assessing of existing tools currently used by the Software Engineering team, for the ability to support our Agile Software Development and system validation and continuous testing; e.g. confirm suitability, identify gaps and make recommendations to address them. • Review Software Engineering processes (requirements, and system test). • Assess existing tools used by Software Engineering, for the ability to support DevOps. • Review current system validation services (system testing and requirements) structure.
Within 90 days of Award	Present findings of the assessment to the OIS Senior Leadership team to include: 1. A detailed action plan (based on analysis) for implementing recommendations of staffing, tool usages for, requirements and system testing, organization structure, testing methodologies, training curriculum and implementation of key performance indicators. 2. Detailed recommendations of transition tasks, activities and timeline, including training plan for new processes that support DevOps tool implementation and Agile Software Development. 3. Recommendations for aligning work teams to DevOps processes and for system validation and continuous testing. 4. Summary recommendations on adopting and implementing industry standard processes and practices, necessary to test IoT, bots, AI and similar technologies.

2.4 Project Milestones

Date	**Milestone**
90 days after award	Presentation of action plan and various recommendations detailed above.

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 may use its personnel or subcontractor personnel to meet the remaining **70%** of the effort.

2.6 Ohio Certified MBE Set-Aside Requirement

None

Section 3: Scope of Work

3.1 Description of Scope of Work

In SCOPE

1. Analysis of software engineering processes. (Requirements, and system test)
2. Deliverable of recommendations for aligning work teams for system validation and continuous testing.

Out of SCOPE

1. Implementation of any processes to support the DevOps team's processes in software engineering.

3.2 Assumptions and Constraints

Assumptions	No additional software or hardware purchases are required.
	The selected Contractor 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 to ODJFS.
	Contractor will provide resources that have in depth experience in DevOps and Agile Software Engineering Processes. Contractor will provide resources that have in depth experience in Agile requirement gathering, software and testing.
Constraints	ODFJS will provide hoteling cubical space for up to five (5) staff at 4200 East Fifth Avenue, Columbus, Ohio 43219.

3.3 Detailed Description of Deliverables

- Deliverables must be provided on the dates specified. Any changes to the delivery date must have prior approval (in writing) by the Agency contract manager or designate.
- All deliverables must be submitted in a format approved by the Agency's 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 Agency 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 Agency contract manager before placed in effect.
- The Agency will complete a review of each submitted deliverable within 10 working days of the date of receipt. A kickoff meeting will be held at 4200 E. Fifth Avenue, Columbus, OH 43215 at a time selected by the Agency where the Contractor and its staff will be introduced to the Agency.

3.4 Deliverables Description

Deliverable Name	**Deliverable Description**
Detailed Project Plan & 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.
Weekly Status Reports	Provide weekly status report of activities for the current week and plans for the next week to include although not limited to schedule changes, staffing changes and outstanding issues that require remediation. At minimum, weekly status reports must contain the items identified below: ▪ Updated Gantt chart, along with a copy of the corresponding Project Plan files (i.e. Microsoft (MS) Project, on electronic media acceptable to the State. ▪ Status of currently planned tasks, including identifying tasks not on schedule and a resolution plan to return to the planned schedule; issues encountered, proposed resolutions and actual resolutions; the results of any tests. The following items must also be included: ♦ A Problem Tracking Report must be attached; ♦ Anticipated tasks to be completed in the next week; ♦ Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones; and ♦ Proposed changes to the Project work breakdown structure and Project schedule. ♦ At a minimum, weekly status reports must contain the following: ▪ A risk analysis of actual and perceived problems; and ▪ Strategic changes to the Project Plan.
Complete findings of the assessment to the OIS Senior Leadership team	1. Complete findings of the assessment to the OIS Senior Leadership team within a three (3) month window of project start to include: a. A detailed action plan (based on analysis) for implementing recommendations of staffing, tool usages, organization structure, testing methodologies, training curriculum and implementation of key performance indicators for system validation and continuous testing. b. Detailed recommendations of transition tasks, activities and timeline, including training plan for new processes that support DevOps implementation and Agile Software Development c. Recommendations for aligning work teams to DevOps processes and for system validation and continuous testing.

Deliverable Name	Deliverable Description
	Summary recommendations on adopting and implementing industry standard processes and practices, necessary to develop and test IoT, bots, AI, and similar technologies.

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
Detailed Project Plan & Schedule		No	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor
Weekly Status Reports	10 days after award	No	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor
Complete findings of the assessment to the OIS Senior Leadership team within a three (3) month window	90 days after award	Yes 100%	Approval from ODJFS Project Manager, technical lead and/or ODJFS Project Sponsor

3.5 Roles and Responsibilities

Project or Management Activity/Responsibility Description	Contractor	Agency
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, reviewing status reports, assisting with project issues 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 five (5) contractor staff members.
ODJFS will provide access to log files and servers necessary to conduct the work.

ODJFS will provide SME for Software Engineering (Development, Requirement, System Testing)

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	Microsoft Project compatible format
Progress Reports	Via email or O365	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 Agency contract manager with *weekly* written progress reports of this project. These are due to the Agency contract manager by the close of business on *the last business day* each week throughout the life of the project.
- The progress reports must cover all work performed and completed during the week for which the progress report is provided and must present the work to be performed during the subsequent week.
- The progress report must 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 must conduct weekly status meetings with the Agency contract manager. The meetings will be held on *Monday* at a time and place so designated by the Agency contract manager – unless revised by the Agency contract manager. The meetings can be in person or over the phone at the discretion of the Agency contract manager.

4.3 Period of Performance

This project is expected to be completed within ninety (90) 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 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	Fee At Risk	Project Completion

	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	Project Completion

4.5 State Staffing Plan

Staff/Stakeholder Name	Project Role	Percent Allocated
ODJFS Staff	Project Manager/Contract Manager	10%
ODJFS Staff	SME for Software Engineering (Development, Requirement, System Testing) and Project Management	10%

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:

- Cover Letter
- Pre-Qualified Contractor Experience Requirements
- Subcontractors Documentation
- Assumptions
- Payment Address
- Staffing plan, personnel resumes, time commitment, organizational chart
- Contingency Plan
- Project Plan
- Project Schedule (WBS using MS Project or compatible)
- Communication Plan
- Risk Management Plan
- Quality Management Plan
- Fee Structure including Estimated Work Effort for each Task/Deliverable
- 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 Pre-Qualified Contractor;

c. Must include a statement regarding the Pre-Qualified 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. Pre-Qualified Contractors Experience Requirements

a. Each proposal must include a brief executive summary of the services the Pre-Qualified 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 Pre-Qualified Contractor's experience, capability, and capacity to provide Information Technology Assessment, Planning, and Solicitation Assistance. 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. **Mandatory Requirements:** The Pre-Qualified Contractor or their subcontractor must possess comprehensive knowledge of project management, conducting IT assessments, strategic and tactical planning, and training development and delivery.

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:

1. Proposed project manager and team members resume or curriculum vitae demonstrating that the team has the necessary professional experience and background.

2. Three references where the proposed project manager has managed a similar project

3. Mandatory Minimum Project Manager Qualifications:
   a) Five (5) years' experience as a project manager developing project plans, defining schedules, developing project approach, budgeting, monitoring and project change management processes.

   b) Minimum seven (7) years' experience in information technology working as a manager, business analyst, systems analyst or programmer.

4. Mandatory Minimum team member experience, this can be multiple resources that have specific skill sets necessary to support the project:
    a) Three (3) years' experience DevOps/Agile development
    b) Three (3) years' experience developing and implementing recommendations of staffing, tool usages for development, requirement and testing methodologies.

2. 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:

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

ii. 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;

iii. 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;

iv. Must describe the Subcontractor's experience, capability, and capacity to provide Information Technology Assessment, Planning, and Solicitation Assistance. 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;

v. A commitment to do the work if the Contractor is selected; and

vi. A statement that the Subcontractor has read and understood the RFP and will comply with the requirements of the RFP.

3. Assumptions: The Pre-Qualified Contractor must list all assumptions the Pre-Qualified Contractor made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the Pre-Qualified 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 Pre-Qualified 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 Pre-Qualified Contractor should not include assumptions elsewhere in their response.

4. Payment Address: The Pre-Qualified Contractor must give the address to which the State should send payments under the Contract.

5.2 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**

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.

5.9 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**
Complete findings of the assessment to the OIS Senior Leadership team		
	Total Cost for all Deliverables	

5.10 Rate Card

Pre-Qualified Contractors must submit a Rate Cards that includes hourly rates for all services the Contractor offers, including but not limited to those listed in Section 5.2. Enter the Rate Cards information in this section.

Section 6: SOW Evaluation Criteria

[Describe SOW Evaluation Criteria. Ensure that all information necessary to complete the evaluation process is requested within Section 5 of this SOW Solicitation Document.

Mandatory Requirements: Accept/Reject

Mandatory Requirements		
Requirement	*Accept*	*Reject*
Prequalified DBITS Contractor – Category Application Development and Maintenance Transition Planning		
Thirty-six (36) months experience DevOps/Agile development		
Thirty-six (36) months experience developing and implementing recommendations of staffing, tool usages for development and testing methodologies.		

Scored Requirements	*Weight*	*Does Not Meet*	*Meet*	*Exceeds*
Contractor or subcontractor shows they have completed similar assessments of software engineering and testing organizations or development organizations that contain an independent software testing groups.	*20*	*0*	*5*	*7*
Contractor or subcontractor must have led the implementation of client adopted, IT-related process improvement recommendations on at least one (1) project.	*10*	*0*	*5*	*7*
Project plan, staffing and timeline proposed demonstrates the ability to complete the project within the desired timeline defined by ODJFS	*10*	*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

[Provide SOW Solicitation Schedule. Add or delete from the sample language, as applicable.]

Firm Dates

SOW Solicitation Released to Pre-qualified Contractors	*June 27, 2018*
Inquiry Period Begins	*June 27, 2018*
Inquiry Period Ends	*July 11, 2018*
Proposal Response Due Date	*July 18, 2018 by 1:00 PM*

Anticipated Dates

Estimated Date for Selection of Awarded Contractor	*August 2018*
Estimated Commencement Date of Work	*August 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 right, select "Bid Opportunities Search";
- Enter the DBITS Solicitation ID number found on the first page of this SOW Solicitation in the "Document/Bid Number:" box;
- Click the "Search" button;
- Click on the Document/Bid Number to go to the document information page,
- On the document information page, click the "Submit Inquiry" button;
- On the 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 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 same instructions described above and by clicking the “View Q & A” button on the document information page.

The State usually responds to all inquiries within three 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.

- 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 business days of receipt, excluding weekends and State holidays. 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 Solicitation.

Section 9: Submission Instructions & Location

Each Pre-Qualified Contractor must submit five (5) complete, sealed and signed copies of its Proposal Response and each submission must be clearly marked “Software Engineering Strategy System Validation and Continuous Testing Project” on the outside of its package along with Pre-Qualified Contractor’s name.

A single electronic copy of the complete Proposal Response must also be submitted with the printed Proposal Responses. Electronic submissions should be on a CD.

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 Pre-Qualified 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 Pre-Qualified Contractors responding to this SOW Solicitation.

Proposal Responses MUST be submitted to the State Agency’s Procurement Representative:

Ohio Department of Job and Family Services
Offices of Contracts and Acquisitions
Software Engineering Strategy System Validation and Continuous Testing Project
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 Pre-Qualified 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 Pre-Qualified 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 Pre-Qualified 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 Pre-Qualified 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 pre-qualified 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

(Identification of Limitation of Liability applicable to the specific SOW Solicitation. 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.

SOW Solicitation Attachments

Attachment Number	Attachment Name/Title
Supplement 1	Security and Privacy
Supplement Addendum revision 1.1	ODJFS -DAS Security Supplement Addendum

Supplement 1: Security and Privacy

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 of 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 agreement;
- 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 agreement. In the event of a conflict for whatever reason, the highest standard contained in this agreement shall prevail.

1. General State Security and Information Privacy Standards and Requirements

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 agreement.

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.
- 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.

- 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.
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies;

a. 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 access or utilize State provided networks, the Contractor is responsible for adhering to State policies and use procedures and do so in a manner as to 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 agreement 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:

- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.

b. Annual Security Plan: State and Contractor Obligations

The Contractor will develop, implement and thereafter maintain annually a Security Plan for review, comment and approval by the State Information Security and Privacy Officer, that a minimum must include and implement processes for the following items related to the system and services:

- Security policies;
  - Application security and data sensitivity classification,
  - PHI and PII data elements,
  - Encryption,
  - State-wide active directory services for authentication,
  - Interface security,
  - Security test procedures,
  - 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:

- Security risks and concerns;

- Application security and industry best practices for the projects; and
- Vulnerability and threat management plan (cyber security).

c. State Information Technology Policies

The Contractor is responsible for maintaining the security of information in environment elements under direct management 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 agreement 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:

- 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 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 Agreements 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.

2. 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.

All parties to this agreement specifically agree 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;
- Corresponding Ohio Administrative Code Rules and Updates; and
- Systems and Services must support and comply with the State's security operational support model which is aligned to NIST 800-53 Revision 4.

d. Protection of State Data

Protection of State Data. To protect State Data as described in this agreement, in addition to its other duties regarding State Data, Contractor will:

- Maintain in confidence any personally identifiable information ("PII") and State Sensitive Information ("SSI") it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Agreement;
- 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 Agreement;
- 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 Agreement 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 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 Agreement;
- 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; and
- 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 or use of PII/SSI.

i. Disclosure

Disclosure to Third Parties. This Agreement 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, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) 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 such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;
- 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.

e. 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 that data from unauthorized disclosure, modification, or destruction. "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. 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.
- 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.

f. 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 data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that 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 the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's 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's 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 erasure, 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 the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's 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's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such 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.
- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's 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.

g. 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 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 agreement.

h. Limited Use; Survival of Obligations.

Contractor may use PII/SSI only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement 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.

i. 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.

j. 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.

k. 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, HIPPA 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.

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.

l. 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 Agreement. "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 (b) 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.

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

m. General

If over the course of the agreement 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 agreement, 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.

n. 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.

o. Unapproved Disclosures and Intrusions: Contractor Responsibilities

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 Agreements 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.

p. 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 and fully cooperate with the State to mitigate the consequences of such a 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 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, 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.

4. Security Review Services

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

q. Application Software Security

The Contractor will:

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

ODJFS -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:

2. A connector that is available within the IBM Identity suite (ISIM) to automate Agency provisioning and de-provisioning tasks.
3. 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 the Ohio Department of Job and Family Services (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.