NOTICE

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

ONLY Contractors pre-qualified in 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.
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
CMA Consulting Services	Persistent Systems
Computer Aid, Inc.	Quantrum LLC
Crowe Horwath LLP	R. Dorsey & Company
CSG Government Solutions	Sense Corp
First Data	Sogeti USA, LLC
Gartner	Sondhi Solutions
HMB, Inc.	System Soft Technologies
IBM	The Greentree Group
IIT Contacts	UMT Consulting
Infojini	Unicon International. Inc.
Information Control Company	Vertex
Information Services Group, Inc.	Wild Goose Enterprises, Inc.

Statement of Work Solicitation

State of Ohio Ohio Department of Job and Family SNAP TANF Data Usage Project Statement of Work	DBITS Solicitation ID No.	Solicitation Release Date
	DBJFS-17-01-001	10-31-2016

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 Contractors:	Monday, October 31, 2016
Inquiry Period Begins:	Monday, October 31, 2016
Inquiry Period Ends:	Thursday, November 10, 2016
Proposal Response Due Date:	Monday, November 21, 2016

Section 2: Background Information

2.1 Agency Information

Agency Name	Ohio Department of Job and Family Services (ODJFS)		
Contact Name	Curt Anderson, Project Manager/Contract Manager	Contact Phone	614.387.8781
Bill to Address	Ohio Department of Job and Family Services (ODJFS) Office of Fiscal and Monitoring Service 30 East Broad Street, 37th floor Columbus, Ohio 43215		

2.2 Project Information

Project Name	SNAP TANF Data Usage
Project Background & Objective	The selected qualified Contractor will conduct a comprehensive assessment of Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF) data that is being collected through various methods and utilized at the State and County level for the Ohio Department of Job and Family Services (ODJFS). The collection of this data is from the operational systems and is being used for reporting and or supporting external systems developed by the County and State users. This assessment does not include evaluation of the content or processes of the ODJFS SNAP and TANF data warehouse, data marts extract and transformations processes. It does include an assessment of the usage of the data marts and COGNOS reporting that is available to State and County users. This project is deliverables based and fixed price. The proposal must include total costs for each deliverable and include travel expenses. ODJFS is transitioning to a new eligibility system called Ohio Benefits to manage the SNAP and TANF programs in July 2017. The Ohio Department of Medicaid has already migrated off of the ODJFS system into Ohio Benefits. The current system, CRIS-e, is the primary data source for the ODJFS Business Intelligence system called the Business Intelligence Channel (BIC). In addition, operational reports are generated through batch processing and are distributed to users through a product called Control-D. It is not known what data State or County users pull out of Control-D and import into other systems. Another area of data usage that is highly dependent on the CRIS-e system are screen scraping utilities that have been implemented by the metro counties. The screen scraping entails running inquiries on case data on a regular basis to extract data that is then used to feed into county developed systems for document management, case management and reporting databases. With the transition to Ohio Benefits, the ability for the counties to use screen scraping will no longer be possible from CRIS-e. This assessment is to document business needs that are being supported through these various activities to determine what the impact will be if the data is no longer available to these users. The expectation is that traditional operational reporting, limited reporting and extract capabilities will be available from Ohio Benefits. SNAP and TANF program data is critical to the daily activities of ODJFS State and County users. At present, program information is gathered by or provided to staff through the following primary channels: • Batch mainframe reports delivered through online viewing software, Control-D • Batch data extract files from the CRIS-E system • “Screen-scraping” or extraction of data from the online CRIS-E system • Interactive Cognos business intelligence reports created from the JFS Data Warehouse • Detail data downloaded from the Cognos business intelligence reports • On-demand data extract files from the JFS Data Warehouse • Direct ad-hoc query access to the JFS Data Warehouse This assessment is not to determine the gap between Ohio Benefits and the need for data by State and County users. The goal is to develop an inventory of what data is being collected, how it’s being collected from CRIS-e, and what is being sourced from the ODJFS data warehouse and data marts for systems and reporting developed by State and County users.
Expected Project Duration	Estimated duration approximately four (4) months. The selected Contractor will be notified by ODJFS when work may begin. The estimated start date for this project is January 9, 2017. This project is expected to be completed within four (4) months after the project start date.
2.3 Project Schedule	

Date	Task
1/9/2017	Project start
1/9/2017	Kickoff meeting
1/16/2017	Meetings with counties scheduled and started
2/27/2017	Survey of counties completed
3/27/2017	Draft document of data usage inventory
4/27/2017	Analysis report completed

2.4 Project Milestones

Date	Milestone
3/27/2017	Completion and Delivery of the Inventory of State and County Data Sources
4/27/2017	Completion and Delivery of the Executive Summary Report
4/27/2017	Completion of Project

2.5 Contractor's Work Effort Requirement

The Contractor's full-time regular employees must perform at least 50% of the effort required to complete the Work. The Contractor may use its personnel or subcontractor personnel to meet the remaining 50% of the effort.

2.6 Ohio Certified MBE Set-Aside Requirement

None

Section 3: Scope of Work

3.1 Description of Scope of Work

The key activities for the Utilization Assessment of SNAP and TANF Program Data include but are not limited to the following:

1. Assess the needs of ODJFS State level stakeholders regarding their business requirements and utilization patterns of SNAP and TANF information from ODJFS information systems for the purpose of managing agency programs, meeting statutory, regulatory and administrative obligations. The groups to be interviewed should include, but may not be limited to the following:
    - The Office of the Director
        - The Office of Policy, Strategy and Performance
        - The Office of Communications
    - The Office of Family Assistance
    - The Office of Fiscal and Monitoring Services
    - The Office of Information Services

Section 3: Scope of Work

2. Assess the needs of ODJFS county level stakeholders regarding their business requirements and utilization patterns of SNAP and TANF information from ODJFS information systems. County assessments must include:
    - On-site visits to a minimum of five (5) county offices
        - Three (3) metro (large, urban) counties
        - Two (2) medium size counties
    - Development of an online survey to be administered to the remaining 83 counties to document their SNAP and TANF program data needs and utilization patterns.
    - Document usage of SNAP and TANF data to create local reports not available from the State operational systems or COGNOS reporting, Business Intelligence Channel (BIC).
    - Document integration of SNAP and TANF data with local systems to improve customer service, drive cost savings, or staff and program performance improvements.
    - Document the impact if this data were not available in the future.

3.2 Assumptions and Constraints

Assumptions	The Contractor has staff with SNAP & TANF program knowledge.
	The Contractor provides technical resources that have experience analyzing data extracts, data integration and developing data attribute definitions and transformation processes documentation.
	The Contractor provides project management and will schedule all meetings at the State and Counties.
	Travel will be required, by the Contractor, to the counties for detail analysis and discussions.
	ODFJS will provide hoteling cubical space at 4200 East Fifth Avenue, Columbus, Ohio 43219 for up to two (2) Contractor staff members.
Constraints	Travel expenses are responsibilities of the Contractor and will not be billed back to ODJFS.
	Requests made to ODJFS staff will be answered within normal business hours. Requests made after hours will be handled next business day.

3.3 Detailed Description of Deliverables

- A kickoff meeting will be held at a location and time selected by the Agency where the Contractor and its staff will be introduced to the Agency.
- 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 contract manager.
- 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 five (5) working days of the date of receipt.

Deliverable Name	Deliverable Description
Detailed Project Plan & Schedule	Provide a detailed project plan and schedule of activities required to complete the assessment
Weekly Status Reports	Provide weekly status report of activities for the current week and plans for the next week
Inventory of State and County Data Sources	Provide an inventory of data sources utilized at the State and County levels that contain, although may not be limited to the following: A. Data source, type of collection (screen scraping, legacy mainframe file, downloaded file share library, downloaded COGNOS generated file, Control-D, etc.). B. Timing and/or schedule that the data is extracted and/or received. C. The system or process the data utilized by. D. Data attributes utilized by the user and or system. E. Business use case description of what the usage is for and how it supports the respective consumer. F. Potential alternative sources for the data if not available from current source. G. Impact if data is no long available.
Survey and Analysis Results Report	Results of survey and analysis and summary of data usage, conclusions and recommendations
Executive Summary Report	An executive report summarizing the findings, patterns, trends, conclusions or recommendations

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
Detailed Project Plan & Schedule		No	Approval from ODJFS Project Manager and/or ODJFS Project Sponsor
Weekly Status Reports		No	Approval from ODJFS Project Manager and/or ODJFS Project Sponsor
Inventory of State and County Data Sources • All county visits are completed. Draft documentation of data usage and collection methods is delivered.	Within 60 days of project start	Yes	Approval from ODJFS Project Manager and/or ODJFS Project Sponsor
Survey and Analysis Results Report		No	Approval from ODJFS Project Manager and/or ODJFS Project Sponsor

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
Executive Summary Report • The completed data usage inventory for County and State level.	Within 120 days of project start	Yes	Approval from ODJFS Project Manager and/or ODJFS Project Sponsor

3.5 Roles and Responsibilities

Project or Management Activity / Responsibility Description	Contractor	Agency
Project Schedule and Deliverables	X	
Providing County and State level contacts		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

- With the exception of the on-site visits to the County offices, on-site work is not a mandatory requirement of this solicitation. However, ODFJS will provide hoteling cubical space, telephones and guest Wi-Fi access at 4200 East Fifth Avenue, Columbus, Ohio 43219 for up to two (2) Contractor staff members.
- ODFJS will provide an Email account for communication and scheduling with County and State staff.

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
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 progress reports of this project. These are due to the Agency contract manager by the close of business on last day of 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 Agency contract manager. The meetings will be held on weekly 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 4 months. 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 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"	Fee At Risk	Monthly
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	Fee At Risk	Monthly

	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"		

4.5 State Staffing Plan

Staff/Stakeholder Name	Project Role	Percent Allocated
Curt Anderson	Project Manager/Contract Manager	10% or As Needed
Larry Lynch	County Relationship Manager – Assists with coordinating county contacts and meeting locations.	10% or As Needed
Bill Ennis	Business Intelligence Manager	20% or As Needed

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. Pre-Qualified Contractor Experience Requirements
3. Subcontractors Documentation

4. Assumptions
5. Payment Address
6. Staffing plan, personnel resumes, time commitment, organizational chart
7. Project Plan
8. Project Schedule (WBS using MS Project or compatible)
9. Communication Plan
10. Fee Structure including Estimated Work Effort for each Task/Deliverable
11. 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 must possess knowledge of conducting comprehensive data assessments and must demonstrate meeting the following:

   - **The Pre-Qualified Contractor must have performed similar work for at least three projects** (including at least one (1) project not performed for ODJFS) within the past five years. **Pre-Qualified Contractors** must demonstrate that they meet this requirement by including a list of at least three references from current or past customers, other than ODJFS, served in the past five years for whom the **Pre-Qualified Contractor** performed similar work. The list must contain current contact persons and contact information for those work engagements. **Pre-Qualified Contractors not meeting this requirement to the satisfaction of ODJFS may be disqualified.** The proposal must contain a brief summary of each of those work engagements, how they are similar in size, scope, and purpose, to the project described in this SOW solicitation document, and the level of success attained.

   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. This must outline how the previous work supported coordinating collecting requirements and specifications from multiple users across geographical sites.

3) Team member(s) have with SNAP & TANF program knowledge.

4) Team members must have experience analyzing business processes that integrate data from multiple sources.

5) Minimum Project Manager Qualifications:

A. Bachelor's Degree in Information Technology or related field or equivalent work experience.

B. Five (5) years' experience as a project manager developing project plans, defining schedules, developing project approach, budgeting, monitoring and project change management processes.

C. Minimum ten (10) years' experience in information technology working as a manager, business analyst, or systems analyst or programmer. Experience with mainframe systems highly desirable.

6) Desirable team member experience;

a. IBM mainframe applications, databases and job control

b. Data warehousing, ETL processes and data quality assessment

c. Business use case and systems design specifications for data integration.

d. Professional certification in BI project management, architecture, ETL, BI reporting internationally recognized BI certification organization (i.e., PMI, TDWI, DAMA, ICCP, Informatica, IBM, Oracle).

ODJFS may disqualify, at its discretion, candidates for whom any of the above requirements are not adequately documented in the Pre-qualified Contractor's proposal.

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:

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 SOW and will comply with the requirements of the Solicitation.

4. 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 Solicitation that the assumption is applicable to. The Pre-Qualified Contractor should not include assumptions elsewhere in their response.

5. Payment Address: The Pre-Qualified 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. 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 in order to meet the final deadline.

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

Describe the Project Schedule including planning, planned vs. actuals for monitoring performance, including milestones, and time for writing, editing and revising. Using MS Project or compatible, 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.

9. Communication Plan

Strong listening skills, the ability to ask appropriate questions, and follow-up questions will be required to capture the information necessary to complete the deliverable requirements. Describe the methods to be used to gather and store various types of information and to disseminate the information, updates, and corrections to previously distributed material. Identify to whom the information will flow and what methods will be used for the distribution. Include format, content, level of detail, and conventions to be used. Provide methods for accessing information between scheduled communications.

10. Fee Structure including Estimated Work Effort for each Deliverable

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

Deliverable Name	Total Estimated Work Effort (Hours)	Not-to-Exceed Fixed Price for Deliverable
Inventory of State and County Data Sources • All county visits are completed. Draft documentation of data usage and collection methods is delivered.		$
Executive Summary Report • The completed data usage inventory for County and State level.		$
	Total Cost for all Deliverables	$

11. Rate Card

The primary purpose of obtaining a Rate Card 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)

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

Section 6: SOW Evaluation Criteria

Mandatory Requirements: Accept/Reject

- Pre-qualified Contractor (and proposed Subcontractor) cover letter(s) included in Section 5.1
- Pre-qualified Contractor submitted properly formatted proposal by submission deadline
- Pre-qualified Contractor possesses knowledge of conducting comprehensive data assessments for at least three projects within the last five years.

Scored Requirements	Weight	Does Not Meet	Meet	Exceeds
Contractor or Subcontractor Summary show(s) company experience in facilitating assessments of data integration and utilization across organizational groups and/or areas.	5	0	5	7
Contractor or Subcontractor Summary identifies resource(s) with SNAP & TANF program knowledge.	3	0	5	7
Contractor or Subcontractor Summary identifies resource(s) that have experience analyzing business processes that integrate data from multiple sources.	7	0	5	7
Contractor or Subcontractor Summary must describe the approach for assessing data usage within an organization.	5	0	5	7
Contractor demonstrates understanding of the requirements detailed in the SOW and the ability to successfully complete and implement them.	5	0	5	7

Scored Requirements	Weight	Does Not Meet	Meet	Exceeds
Pre-qualified Contractor(s) staffing plan.	3	0	5	7
Demonstrated ability to complete the project in the available timeline based on the proposed project plan.	3	0	5	7
Pre-qualified Contractor(s) communication plan.	3	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 Pre-qualified Contractors	Monday, October 31, 2016
Inquiry Period Begins	Monday, October 31, 2016
Inquiry Period Ends	Thursday, November 10, 2016
Proposal Response Due Date	Monday, November 21, 2016; no later than 1:00 PM

Anticipated Dates

Estimated Date for Selection of Awarded Contractor	Monday, December 5, 2016
Estimated Commencement Date of Work	Monday, January 9, 2017

All times listed are Eastern Standard Time (EST).

Section 8: Inquiry Process

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

- Access the State's Procurement Website at http://procure.ohio.gov/;
- From the Quick Links bar on the right, select "Bid Opportunities Search";
- Enter the DBITS Solicitation ID number found on the first page of this SOW Solicitation;
- Click the "Search" button;
- In the Other section, click the "Submit Inquiry" button;
- On the document inquiry page, complete the required "Personal Information" section by providing:
    - First and last name of the Pre-Qualified Contractor's representative who is responsible for the inquiry,
    - Name of the Pre-Qualified 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
- Type the Security Number seen on the right into the Confirmation Number; and
- Click the "Submit" button.

A Pre-Qualified 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.

Pre-Qualified Contractors may view inquiries and responses on the State's Procurement Website by using the "Find It Fast" 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. 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 Pre-Qualified Contractor must submit THREE (3) complete, sealed and signed copies of its Proposal Response and each submission must be clearly marked "SNAP TANF Data Usage " 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, 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 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.

As noted in section 7 Submission calendar of events proposals are due on Monday, November 21, 2016; no later than 1:00 PM. 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
ATTENTION: CURT ANDERSON
30 East Broad Street, 31st floor
Columbus, Ohio 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.

Supplement 1

Supplement: Security and Privacy

State of Ohio Department of Administrative Services / Office of Information Technology

Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

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;

1.1. 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.

1.2. 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).

1.3. 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.

2.1. 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:
  a) Security and confidentiality of PII/SSI;
  b) Protection against anticipated threats or hazards to the security or integrity of PII/SSI; and
  c) Protection against the unauthorized access or use of PII/SSI.

2.1.1. 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.

2.2. 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.

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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

3.1. 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.

3.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any 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.

3.3. 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.

3.4. 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:

4.1. 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.