

NOTICE

This opportunity is being released to Deliverable Based IT Services (DBITS) Contractors pre-qualified as a result of Minority Business Enterprise (MBE) RFP #0A1139.

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 submitted by organizations not pre-qualified in this Technology Category.

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

1. Advocate Technical Services
2. American Business Solutions
3. Ardent Technologies Inc.
4. CDO Technologies, Inc.
5. Cluster Software, Inc.
6. CompTech Computer Technologies
7. Digitek Software, Inc.
8. Diversified Systems, Inc.
9. Evanhoe & Associates
10. Fine Citizens
11. Flairsoft
12. Halcyon solutions, Inc.
13. Logic Soft, Inc.
14. Optimum Technology
15. Proteam Solutions, Inc.
16. Sophisticated Systems, Inc.
17. Srisys, Inc.
18. Stellar Innovations & Solutions, Inc.
19. Strategic System's Inc.
20. TMH Solutions
21. Unicon International, Inc.
22. Vana Solutions
23. Ventech Solutions, Inc.
24. Vertex

Statement of Work Solicitation

	OhioMHAS Community Transition Program (CTP)	DBITS Solicitation ID No.	Solicitation Release Date
		DBDMH-16-03-001	1-11-2016

Section 1: Purpose

The purpose of this Project Statement of Work (SOW) is to provide the Ohio Department of Mental Health, with information technology services in Applications Development and Maintenance Transition Planning Technology Category. The State is seeking a Pre-qualified Contractor, herein after referred to as the “Contractor”, to 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

- Section 1: Purpose
- Section 2: Background Information
- Section 3: Scope of Work
- Section 4: Deliverables Management
- Section 5: SOW Response Submission Requirements
- Section 6: SOW Evaluation Criteria
- Section 7: SOW Solicitation Schedule
- Section 8: Inquiry Process
- Section 9: Submission Instructions & Location
- Section 10: Limitation of Liability

Timeline

- Firm Dates
- SOW Solicitation Released to Pre-qualified Contractors: January 11, 2016
- Inquiry Period Begins: January 11, 2016
- Inquiry Period Ends: January 15, 2016 8 a.m.
- Proposal Response Due Date: January 19th, 2016 at 4 p.m.

Section 2: Background Information

2.1 Agency Information

Agency Name	Department of Mental Health Addiction Services (OhioMHAS)		
Contact Name	Jody Lynch	Contact Phone	614-466-5908
Bill to Address	Department of Mental Health Addiction Services (OhioMHAS)		

2.2 Project Information

Project Name	Department of Mental Health Addiction Services (OhioMHAS) Community Transition Program (CTP)
Project Background & Objective	<p>These Business Requirements are for the Ohio Department of Mental Health Addiction Services (OhioMHAS) Community Transition Program (CTP) to capture and manage the data of applicants (coordinating entities) who will work in collaboration with partners from surrounding communities and across board and agency boundaries to successfully transition incarcerated selected individuals with substance use disorders back to their community.</p> <p>Many individuals incarcerated within Ohio Department of Rehabilitation and Correction (ODRC) institutions have histories of addiction and have participated in treatment programs within the Bureau of Recovery Services located in the institutions. The Community Transition Program (CTP) is designed to improve access to treatment and recovery support services for individuals that received Substance Use Disorders (SUD) programming while incarcerated as they transition to the community. Coordinating entities shall work in collaboration with partners from surrounding communities to successfully transition incarcerated individuals</p> <div data-bbox="488 768 1373 1125" data-label="Diagram"> <pre> graph TD Admin[OhioMHAS Administrator] R1[Region 1 Coordinating Entity] R2[Region 2 Coordinating Entity] R3[Region 3 Coordinating Entity] R4[Region 4 Coordinating Entity] R5[Region 5 Coordinating Entity] R6[Region 6 Coordinating Entity] Admin --- R1 Admin --- R2 Admin --- R3 Admin --- R4 Admin --- R5 Admin --- R6 </pre> </div> <p>back to their community.</p> <p>The OhioMHAS shall act as the application administrator and will be responsible to monitor and manage the progress of the CTP program. The OhioMHAS Community Transition Project (CTP) system will be used by the coordinating entities (six Ohio regions) to input treatment data aggregated from the providers who are directly providing treatment services to the clients in transition. By aggregating data from the provider and entity coordinators, the OhioMHAS Administrator will be able to track, manage, and report on the usage and effectiveness of the CTP Program</p>
Expected Project Duration	Date of executed contract to Jan 22, 2016. All work and project acceptance must be completed by March 15, 2016 and paid out no later than June 30, 2016.
2.3 Project Schedule	
Date	Task
1/25/2016	Project Start Date
1/25/2016	Initial Project kick off meeting

Date	Task
1/27/2016	Functional Design and Technical Design Documents acceptance
1/29/2016	Project Plan acceptance
2/22/2016	Development complete
2/29/2016	UAT Begin date
3/4/2016	UAT sign off
3/11/2016	Delivery of tasks detailed in the Scope of Work including documentation.
3/15/2016	Project sign off, acceptance, and completion

2.4 Project Milestones

Date	Milestone
Within 2 business days of contract award	Initial kick off meeting with OhioMHAS and Contractor.
Within 4 business days of initial kick off meeting	Business and Functional Requirements document review and acceptance by OhioMHAS.
Within 2 business days of Business Requirements acceptance	Project Plan review and acceptance by OhioMHAS.
Determined in project plan	Review and acceptance of Functional Design and Technical Design Documents.
Determined in project plan	Review and acceptance of Test Plan.
Determined in project plan	Review and acceptance of Working Code.
Determined in project plan	Review and acceptance of User Manual.
Determined in project plan	Review and acceptance of Technical Documentation

Determined in project plan but no later than 3/15/2016	Project sign off, acceptance, and completion.
--	---

2.5 Contractor’s Work Effort Requirement

The Contractor’s full-time regular employees must perform at least 35% of the effort required to complete the Work. The Contractor may use its personnel or subcontractor personnel to meet the remaining 65% of the effort.

2.6 Ohio Certified MBE Set-Aside Requirement

The SOW Solicitation is a MBE Set-Aside opportunity.

Section 3: Scope of Work

3.1 Description of Scope of Work

Technical Development (system programming) – This project must be written utilizing a MVC5 architecture in C# and Microsoft SQL Server, the Contractor must have expert level knowledge of these platforms .

Project Management - The Contractor must provide Project Management for the duration of the project. The Contractor must adhere to the accepted Project Plan and provide Weekly Status Reports that document at a minimum the progress, issues and next steps for the project. Additionally, the Contractor must provide OhioMHAS with a not to exceed fixed price per deliverable; a payment schedule tied to proposed project milestones and acceptance of each deliverable; and maintain logs for project issues and risks.

Use of OhioMHAS / ITG PMBOK forms, templates, or documents is acceptable and will be provided upon request. Contractor forms, templates, or project documentation based on PMBOK methods is also acceptable.

Application Requirements – Detailed requirements for the OhioMHAS Community Transition Program are contained in the following attachments:

- OhioMHAS CTP Data Elements Table (Attachment A)
- OhioMHAS CTP User Roles & Responsibilities (Attachment B)
- OhioMHAS CTP Business and Functional Requirements (Attachment C)
- OhioMHAS CTP Additional Requirements (Attachment D)
- OhioMHAS CTP Reports (Attachment E)
- OhioMHAS CTP Entity Diagram (Attachment F)
- Security Supplement (Supplement 1)

3.2 User Interface Features

Every screen must follow consistent aesthetic standards that must include attributes such as:

The fields used in all forms shall be wide enough to accommodate at least 95% of expected entries without requiring either horizontal or vertical scrolling, except for fields whose input exceeds 10 words, where vertical scroll bars shall become enabled if the user enters enough information to force a line break

For fields of known maximum length, such as the 10 characters of postal code (ZIP+4, plus hyphen), the fields shall not be wider than necessary to contain the expected entries.

Each page in the website shall have a menu bar with links to the major pages (major pages being defined as the home page and those other pages directly accessible from the home page). The menu options shall change font color, style, and/or size when the user hovers

Section 3: Scope of Work

their mouse pointer over them. If the currently displayed page appears in the menu bar, its link shall be shown in a different font color than the other menu options.

When processing of a script is completed, the web page shall display either a message confirming that the form information was submitted correctly or a descriptive error message if an error occurred during script processing.

The State may provide Contractor with the Cascading Style Sheets (CSS) for the Web Design Standards.

3.3 Due to the nature of work contained in this Statement of Work, additional Security and Privacy requirements are contained in Supplement 1. The Contractor must accept and meet these requirements.

3.4 Assumptions and Constraints

Assumptions	Web based application for remote access and usage
	Client records may include HIPAA or Protected Health Information (PHI)
	Brand new system supporting a new program
	There will be no legacy data to import
	Six regions with users will need to access the system
	Anticipate 5,000+ clients (clients) per year
	Data will not be used for claims processing or payment (no funding information will be included)
Constraints	Contractors must work on-site at the location described in section 3.8.

3.5 Detailed Description of Deliverables

- Deliverables must be provided on the dates specified in the accepted project plan. 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 and 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 which cannot exceed Feb 29, 2016. 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 5 working days of the date of receipt.

- 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.

Deliverable Name	Deliverable Description
Project Plan for the CTP Application	The project plan shall include a proposed project schedule, project budget, status reports, and documentation on issues (log), risks, and assumptions. The detailed project schedule shall align with the mandatory project sign off and completion date of March 15, 2016.
Finalized Functional and Business Requirements Document for CTP	The documentation for this deliverable shall clearly verify final, Functional and Business Requirements based on analysis of the detailed requirements and discussions with the SMEs.
Functional Design and Technical Design Documents	This documentation will include finalized design documents for the CTP Application.
Test Plan	This documentation shall include a detailed Test Plan for UAT
Test Plan Results	Publish test results (UAT of Test Plan) Review and acceptance UAT including load and performance testing.
Working Code	Delivery of the production source code for the CTP Solution.
User Manual and Technical Documentation	Provide User Manual and Technical Documentation for review and acceptance. The User Manual should include each role identified in Attachment B. Technical Documentation must fully document the solution and provide adequate detail for State staff to support the application.

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
Project Plan	Within the Scope of the Project Timeline	No	Agency approval of deliverable
Finalized Functional and Business Requirements Document for CTP	Determined in Approved Project Plan	No	Agency approval of deliverable
Functional Design and Technical Design Documents	Review and acceptance of FDD and TDD	No	Agency approval of all FDD and TDD tasks
Test Plan	Review and acceptance of	Yes – 25% of the not-to-exceed fixed	Agency approval of all Testing and regression tasks

Deliverable Name	Due Date (If applicable)	Payment Eligible? Yes/No	Acceptance Criteria
	determined in project plan.	price and approval of deliverables listed above.	
Test Plan Results	Determined in project plan	No	Agency approval UAT
Working Code	Determined in project plan.	Yes – 40% of the not-to-exceed fixed price with approval of Test Plan Results and Working Code.	Agency approval of all code promotion tasks
User Manual and Technical Documentation	Determined in project plan	No	Agency approval of User Manual and Technical Documentation.
Project sign off and completion	March 15, 2016	Yes – remaining 35% of the not-to-exceed fixed price.	Completion of Agency testing for full system and acceptance of all deliverables.

3.6 Roles and Responsibilities

Project or Management Activity / Responsibility Description	Contractor	Agency
Provide funding, documentation, feedback, availability, and approval for the success of the Statement of Work.		X
Provide appropriate access.		X
OhioMHAS will have environments ready prior to the start of the project.		X
OhioMHAS/ITG will make its project manager and other necessary personnel available to the Contractor's project manager and team members to fully acquaint them with the OhioMHAS IT environment. A contact person will be named who will be OhioMHAS's principal agent with respect to all technical issues involved in the project. OhioMHAS / ITG will provide the		X

Project or Management Activity / Responsibility Description	Contractor	Agency
Contractor with telephone number and e-mail address for this contact person, and a backup to cover for the contact person in the event the contact person is absent from work.		
OhioMHAS/ITG will provide virtual server environments for the completion of this work. Additional software tools will be provided to successfully complete the assigned duties. These environments cannot be accessed remotely and must be accessed from a State controlled facility.		X
Provide deliverables specified in the Statement of Work Solicitation	X	
Report all issues that may impact the project timeline in writing to OhioMHAS.	X	
Provide weekly status reports to OhioMHAS and updated project schedules as appropriate. While required, Project Management artifacts are not eligible for payment. Costs related to Project or Management Activity/Responsibility must be included in the proposed deliverable.	X	
Contractor must provide personnel to be on-site as needed.	X	

3.7 Restrictions on Data Location and Work

The State requires the development efforts to be performed on-site. 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.

3.8 Resource Requirements

OhioMHAS will provide workspace on the 19th floor of the Rhodes Tower located at 30 East Broad Street, Columbus, OH 43215; Franklin County.

OhioMHAS expects the Contractor will provide all of the necessary personnel and equipment to successfully complete the work specified in this Statement of Work Solicitation.

OhioMHAS will maintain virtual server environments prior to the project start date and thereafter.

Contractor is required to work with OHIOMHAS and DAS staff. OhioMHAS and DAS normal working hours are 8:00am to 5:00pm with a one-hour lunch period for a total of eight working hours per day. Contractor may have to work under unusual working conditions which may include operation of a computer terminal for long periods of time, working in excess of eight hours per day, working on Saturdays and/or Sundays.

Section 4: Deliverables Management

4.1 Submission/Format

PM Artifact/Project Work Product	Submission	Format
---	-------------------	---------------

Project Plan for the CTP Application	E-mail and specified SharePoint location	Microsoft Project
Finalized Functional and Business Requirements Document for CTP	E-mail and specified SharePoint location	Microsoft Word or PDF
Weekly Status Reports	E-mail and specified SharePoint location	Microsoft Word or PDF
Functional Design and Technical Design Documents	E-mail and specified SharePoint location	Microsoft Word or PDF
Test Plan	E-mail and specified SharePoint location	Microsoft Word or PDF
Test Plan Results	E-mail and specified SharePoint location	Microsoft Word or PDF
Working Code	FTP	MVC5 and SQL Server
User Manual and Technical Documentation	E-mail, specified SharePoint location and hardcopy original	Microsoft Word or PDF

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 Monday 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 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

The period of performance will last from the date of executed contract thru March 15, 2016 or until all of the deliverables are completed, accepted, and delivered.

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
<p>Delivery Date Service Level</p>	<p>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.</p> <p style="text-align: center;">Compliance with delivery date is expected to be greater than 85%</p> <p>This SLA is calculated as follows: “% Compliance with delivery dates” equals “(Total dates in period – Total dates missed)” divided by “Total dates in period”</p>		
<p>Deliverable Acceptance Service Level</p>	<p>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</p>		

	<p>will run continuously thereafter until the expiration of the applicable SOW.</p> <p style="text-align: center;">Compliance with deliverable acceptance is expected to be greater than 85%</p> <p>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”</p>		
<p>Scheduled Reports Service Level</p>	<p>The Scheduled Reports Service Level will measure the receipt of Reports within Project schedule or other established time frames.</p> <p>This SLA is calculated as follows: “Scheduled Reporting Performance” equals “(Total Number of Reports Required – Total Reports Missed/Missing)” divided by “Total Number of Reports Required”</p>		
<p>System Test Execution Exit Quality Rate</p>	<p>The System Test Execution Exit Quality Rate will, prior to UAT, be determined using the results of Contractor generated pre-test strategy, executed testing cases including functionality, performance, integration, interfaces, operational suitability and other test coverage items comprising a thorough Contractor executed system testing effort. Regression Testing must be performed as necessary. “System Test Execution Exit Quality Rate” means the inventory of all test cases performed in conjunction with Contractor system testing, or testing otherwise preceding the State’s User Acceptance Testing efforts, presentation of resultant test performance inclusive of identified errors or issues (by priority), impact areas and overall testing results to the State otherwise referred to as “Testing Results”.</p> <p>This Service Level begins upon Contractor presentation of the aforementioned Testing Results to the State prior to the State conducting UAT. The initial service level shown for this SLA will be 90.0%, exclusive of Critical and High defects (which must be resolved prior to presentation to the State) and will be</p>		

	<p>validated during an initial measurement period. The initial and subsequent measurement periods will be as mutually agreed by the Parties. Following the initial measurement period, and as a result of any production use the Service Level will be adjusted to 95%.</p> <p>Compliance with the System Test Execution Exit Quality Rate is expected to be greater than or equal to 90% prior to UAT and greater than or equal to 95% in production</p> <p>This SLA is calculated as follows: “System Test Quality/Exit Rate” equals “Total Test Cases Passing Contractor System Test Efforts” divided by “Total Executed during System Testing Effort”</p>		
<p>Mean Time to Repair/Resolve Critical Service Level</p>	<p>The Mean Time to Repair/Resolve Critical Service Level will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all in-scope Critical Defect service requests in the Contract Month. “Time to Repair” is measured from time a Defect is received by the Contractor to point in time when the Defect is resolved by the Contractor and the Contractor submits the repair to the State for confirmation of resolution. “Critical Defect Service Request” affects critical functionality or critical data. No work-around exists.</p> <p>* In lieu of any specifically stated SLA determined by the project sponsor, the default requirement shall apply.</p> <p>Mean Time to Repair/Resolve pre-implementation Critical Defects is expected to be less than or equal to 24 hours*</p> <p>Mean Time to Repair/Resolve post-implementation Critical Defects is expected to be less than or equal to 24 hours</p> <p>This SLA is calculated as follows: “Mean Time to Repair/Resolve (Critical Defects)” equals “Total elapsed time it takes to repair Critical Defect Service Requests” divided by “Total Critical Defect Service Requests”</p>		
<p>Mean Time to Repair/Resolve High Service Level</p>	<p>The Mean Time to Repair/Resolve High Service Level will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all in-scope High Defect service requests in the Contract Month. “Time to</p>		

	<p>Repair” is measured from time a Defect is received by the Contractor to point in time when the Defect is resolved by the Contractor and the Contractor submits the repair to the State for confirmation of resolution. “High Defect Service Request” affects critical functionality, but there is a temporary work-around however it is difficult to implement.</p> <p>Mean Time to Repair/Resolve pre-implementation High Defects is expected to be less than or equal to 72 hours</p> <p>Mean Time to Repair/Resolve post-implementation High Defects is expected to be less than or equal to 72 hours</p> <p>This SLA is calculated as follows: “Mean Time to Repair/Resolve (High Defects)” equals “Total elapsed time it takes to repair High Defect Service Requests” divided by “Total High Defect Service Requests”</p>		
<p>Mean Time to Repair Medium Service Level</p>	<p>The Mean Time to Repair Medium Service Level will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all in-scope Medium Defect service requests in the Contract Month. “Time to Repair” is measured from time a Defect is received by the Contractor to point in time when the Defect is resolved by the Contractor and the Contractor submits the repair to the State for confirmation of resolution. “Medium Defect Service Request” affects minor functionality or non-critical data. There is an easy, temporary work-around.</p> <p>Mean Time to Repair/Resolve pre-implementation Medium Defects is expected to be less than or equal to 7 calendar days</p> <p>Mean Time to Repair/Resolve post-implementation Medium Defects is expected to be less than or equal to 7 calendar days</p> <p>This SLA is calculated as follows: “Mean Time to Repair/Resolve (Medium Defects)” equals “Total elapsed time it takes to repair medium Defect Service Requests” divided by “Total Medium Defect Service Requests”</p>		

4.5 State Staffing Plan

Staff/Stakeholder Name	Project Role	Percent Allocated
Jody Lynch	OhioMHAS Sponsor	As Needed
Rosemary Tolliver	OhioMHAS SME	As Needed
Chris Nicastro	OhioMHAS Business Owner	As Needed

Staff/Stakeholder Name	Project Role	Percent Allocated
Glen Coleman	DAS OIT SME	As Needed
Venu Edupuganti	DAS OIT Project Manager	As Needed
Tom Denegre	DAS OIT Business Analyst	As Needed
Eric Frick	DAS OIT Service Owner	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:

- Cover Letter
- Pre-Qualified Contractor Qualifications Summary
- 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
- Rate Card

1. Cover Letter:

- a. Must be in the form of a standard business letter;
- b. Must be signed by an individual authorized to legally bind the Contractor;
- c. Must include a statement regarding the Contractor's legal structure (e.g. an Ohio corporation), Federal tax identification number, and principal place of business; please list any Ohio locations or branches;
- d. Must include a list of the people who prepared the Proposal, including their titles; and
- e. Must include the name, address, e-mail, phone number, and fax number of a contact person who has the authority to answer questions regarding the Proposal.

2. Pre-Qualified Contractor Qualifications Summary:

- a. Must include an executive summary of the services the Contractor proposes to provide and three representative references of previously completed projects that demonstrate knowledge and execution of the required technologies and methodologies required in this project (e.g. description of similar projects completed utilizing Business Analysis, information technology application development integration with MVC5, C#, and SQL Server)
- b. Must describe the Contractor's experience, capability, and capacity to complete the application development services required. Provide specific detailed information demonstrating experience similar in nature to the type of work described in this SOW for each of the resources identified in Section 5.2.

3. 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. Must include a brief executive summary of the services the Subcontractor proposes to provide and three representative references of previously completed projects that demonstrate knowledge and execution of the required technologies and methodologies required in this project (e.g. description of similar projects completed utilizing Business Analysis, information technology application development with MVC5, C#, and SQL Server)
 - iv. Must describe the Subcontractor’s experience, capability, and capacity to complete the application development services required. 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. Must include an executive summary of the services the Subcontractor proposes to provide and three representative references of previously completed projects that demonstrate knowledge and execution of the required technologies and methodologies in application integration.
 - vi. A commitment to do the work if the Subcontractor is selected; and
 - vii. A statement that the Subcontractor has read and understood the RFP and will comply with the requirements of the RFP.

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

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

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.

Staffing plan shows individual skills in SQL Development, 5 years project management, C# and MVC5.

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 Sub-Contractor 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 in order to meet the final deadline.

5.5 Project Schedule (WBS using MS Project or compatible)

Describe the Project Schedule including planning, defining goals, 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.

5.6 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.

5.7 Risk Management Plan

Describe the Risk Management Plan requirements including the risk factors, associated risks, and assessment of the likelihood of occurrence and the consequences for each risk. Describe your plan for managing 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 application enhancements.

5.9 Fee Structure including Estimated Work Effort for each Task/Deliverable

The Contract award will be for a not to exceed fixed price.

Payment will be scheduled upon approval & acceptance of milestones and deliverable described below.

- Payment of 25% of the total not-to-exceed fixed price of all deliverables will be paid upon acceptance of **ALL** the following deliverables:
 - Project Plan
 - Finalized Functional and Business Requirements Document for CTP
 - Functional Design and Technical Design Documents
 - Test Plan
- Payment of 40% of the total not-to-exceed fixed price of all deliverables will be paid upon acceptance of **ALL** the following deliverables:
 - Test Plan Results
 - Working Code
- Final payment of the remaining 35% of the total not-to-exceed fixed price of all deliverables will be paid at the Project sign off and completion.

Deliverable Name	Total Estimated Work Effort (Hours)	Not-to-Exceed Fixed Price for Deliverable
Project Plan for the CTP Application		
Finalized Functional and Business Requirements Document for CTP		
Functional Design and Technical Design Documents		
Test Plan		
Working Code		
User Manual and Technical Documentation		
TOTAL COST FOR PROJECT		\$

5.10 Rate Card

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

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				
<ul style="list-style-type: none"> Pre-qualified Contractor or Subcontractor cover letter(s) included in Section 5.1 Pre-qualified Contractor or Subcontractor(s) submitted properly formatted proposal by submission deadline 				
	Weight	Does not meet	Meet	Exceeds
Scored Criteria 6.1 Contractor or Subcontractor Summary show(s) company experience in information technology application development utilizing: <ul style="list-style-type: none"> Microsoft C# Microsoft SQL Server MVC3 Architecture or higher 	3	0	5	7

6.2 Contractor or Subcontractor Documentation shows resource(s) identified in Section 5.2 experience in information technology application development utilizing: <ul style="list-style-type: none"> • Microsoft C# • Microsoft SQL Server • MVC3 Architecture or higher 	10	0	5	7
6.3 Contractor or Subcontractor Summary must describe how they meet the following skills through described implemented examples of work performed. <ul style="list-style-type: none"> • Business Analysis • Successful completion of C# application coding • SQL Database development 	3	0	5	7
6.4 Contractor must demonstrate understanding of the requirements detailed in the SOW and the ability to successfully complete and implement them.	3	0	5	7
6.5 Pre-qualified Contractor(s) staffing plan shows 5 years project management experience with application development.	4	0	5	7
6.6 Pre-qualified Contractor(s) staffing plan shows individual application development and programming language skills in C#.	6	0	5	7
6.7 Pre-qualified Contractor(s) staffing plan shows individual skills in SQL database development.	6	0	5	7
6.8 Pre-qualified Contractor(s) contingency plan	5	0	5	7
6.9 Contractor must demonstrate ability to complete the project in the available timeline based on the proposed project plan.	5	0	5	7
6.10 Pre-qualified Contractor(s) communication plan.	2	0	5	7
6.11 Pre-qualified Contractor(s) risk management plan	2	0	5	7
6.12 Pre-qualified Contractor(s) quality management plan	4	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:

$$\text{Technical Proposal Points} = \left(\frac{\text{Offeror's Technical Proposal Points}}{\text{Highest Number of Technical Proposal Points Obtained}} \right) \times 700$$

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:

$$\text{Cost Summary Points} = \left(\frac{\text{Lowest Total Cost for Evaluation Purposes}}{\text{Offeror's Total Cost for Evaluation Purposes}} \right) \times 300$$

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

$$\text{Total Points} = \text{Technical Proposal Points} + \text{Cost Summary Points}$$

Section 7: SOW Solicitation Calendar of Events

Firm Dates

SOW Solicitation Released to Pre-qualified Contractors	January 11, 2016
Inquiry Period Begins	January 11, 2016

Inquiry Period Ends	January 15, 2016 at 8 a.m.
Proposal Response Due Date	January 19, 2016 at 4:00 p.m.

Anticipated Dates

Estimated Date for Selection of Awarded Contractor	January 22, 2016
Estimated Commencement Date of Work	February 27, 2016

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 6 complete, sealed and signed copies of its Proposal Response and each submission must be clearly marked "CONFIDENTIAL – OhioMHAS SOW DBITS SOLICITATION ID NO. DBDMH – 16 – 03 - 001" 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.

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

Venu Edupuganti
Department of Medicaid
Lazarus Building (reception area)
50 West Town Street
Columbus, OH 43215

Deliveries will be accepted Monday through Friday 8:00AM and 4:00PM excluding holidays.

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
A	OhioMHAS CTP Data Elements Table
B	OhioMHAS CTP User Roles & Responsibilities
C	OhioMHAS CTP Business and Functional Requirements
D	OhioMHAS CTP Additional Requirements
E	OhioMHAS CTP Reports
F	OhioMHAS CTP Entity Diagram
SUPPLEMENT 1	Security Supplement

A - OhioMHAS CTP Data Elements Table

ID	Table	Field Name	Attribute	Required	Comments
1	User Registration	UserID	Integer	Yes	System generated Unique key record
2	User Registration	User_Name	vchar(50)	Yes	State users will use their State UserID. Remote users will NOT use their email address. Must be a unique system name.
3	User Registration	Region	Text	Yes	Dropdown values Akron Dayton Cincinnati Cleveland Columbus Lima OhioMHAS
4	User Registration	Organization_Name	vchar(50)	Yes	
5	User Registration	Last_Name	vchar(50)	Yes	
6	User Registration	First_Name	vchar(30)	Yes	
7	User Registration	Email	vchar(50)	Yes	
8	User Registration	Telephone	Number	Yes	Format XXX_XXX_XXXX
9	Client	ClientID	Number	Yes	Key Record_Unique identifier Start Key # at CTP100001
10	Client	Client DRC Inmate Number	Varchar (15)		
11	Client	Client_SSN	Number		Format XXX_XXX_XXXX
12	Client	Client Medicaid Number	vchar(10)	No	Medicaid_unique number in system
13	Client	Client In Reach Date	Short Date	Yes	MM_DD_YYYY
14	Client	Client Start Date	Short Date	Yes	MM_DD_YYYY
15	Client	Client Modified Date	Short Date	Yes	MM_DD_YYYY System generated
16	Client	CTP Discharge Date	Short Date		MM_DD_YYYY
17	Client	Client_Last_Name	vchar(30)	Yes	
18	Client	Client_First_Name	vchar(30)	Yes	
19	Client	Client_Adress	vchar(40)	Yes	

ID	Table	Field Name	Attribute	Required	Comments
20	Client	Client_City	vchar(30)	Yes	
21	Client	Client_State	char(2)	Yes	
22	Client	Client_Zip	Number		Zipcode format
22.1	Client	ClientCounty	Text	Yes	Drop Down Values Use County Table to select values
22.2	Client	ClientRegion	Text	Yes	System populates region based on county selection
23	Client	Client_Telephone	Number	Yes	Format XXX_XXX_XXXX
24	Client	Client Email	vchar(50)		
25	Client	Client_Birthdate	Short Date	Yes	MM_DD_YYYY
26	Client	Emergency Contact First Name	vchar(30)	Yes	
27	Client	Emergency Contact Last Name	vchar(30)	Yes	
28	Client	Emergency Contact Address	vchar(40)	Yes	
29	Client	Emergency Contact City	vchar(30)	Yes	
30	Client	Emergency Contact ST	char(2)	Yes	
31	Client	Emergency Contact Zip	Number		Zipcode format
32	Client	Emergency Contact Telephone	Number		Format XXX_XXX_XXXX
33	Client	Emergency Contact Relationship	vchar(50)		
34	Client	On PRC	Bit	Yes	Yes/No
35	Client	Managed Care Plan Name	vchar(50)	Yes	Drop Down Values Buckeye Caresource Molina Paramount United
36	Client	Medicaid Application Submitted	Bit		Select_Yes/No (Default = No)
37	Client	Medicaid Eligibility Start Month	Short Date		MM_YYYY
38	Client	Client Status	Text	Yes	Drop down Values Enrolled Discharged
39	Client	Gender	Text	Yes	Drop down values Male Female

ID	Table	Field Name	Attribute	Required	Comments
40	Client	Race	Text	Yes	Drop Down Values White Black/African American Hispanic/Latino Asian Native Hawaiian/Pacific Islanders American Indian/Alaskan Native
41	Client	Prison Release Date	Short Date	Yes	MM_DD_YYYY
42	Client	Prison Release Type	Text	Yes	Drop Down Values Detainer EDS EST Judicial Release Parole PRC Transitional Control Other
43	Client	Releasing Prison	Text	Yes	Drop Down Values Use Prison Table to select values
44	Client	County of Release	Text	Yes	Drop Down Values Use County Table to select values
45	Client	Housing Type	Text	Yes	Drop Down Values Adult care facility Halfway House Homeless Independent Housing Nursing Home Permanent Supportive Housing Transitional Facility (shelter, homeless facility)
46	Client	Insurance Type	Text	Yes	Drop Down Values Medicaid Private Military Medicare Other Uninsured
47	Client	Client Notes	Text		
48	Record	RecordID	Number	Yes	Key record for unique Record ID

ID	Table	Field Name	Attribute	Required	Comments
49	Record	Record_Date	Short Date	Yes	MM_DD_YYYY
50	Record	Fiscal Year	Number	Yes	System auto-calculates Fiscal year based on Record_Date
51	Record	Service_Region	Text	Yes	Dropdown values Lima Dayton Cincinnati Columbus Cleveland Akron
52	Record	Treatment_Diagnostic Assessment	Integer		PROVIDED SERVICE
53	Record	Treatment_Intensive outpatient services	Integer		PROVIDED SERVICE
54	Record	Treatment_Urinalysis	Integer		PROVIDED SERVICE
55	Record	Treatment_Outpatient Treatment	Integer		PROVIDED SERVICE
56	Record	Treatment_Community Residential Treatment	Integer		PROVIDED SERVICE
57	Record	Treatment_Case Management	Integer		PROVIDED SERVICE
58	Record	Treatment_Medication assisted Treatment	Integer		PROVIDED SERVICE
59	Record	Treatment_Crisis Intervention	Integer		PROVIDED SERVICE
60	Record	Treatment_Ambulatory detoxification services	Integer		PROVIDED SERVICE
61	Record	Treatment_Other services	char (100)		PROVIDED SERVICE Brief description of services
62	Record	Recovery_Recovery Housing	Integer		PROVIDED SERVICE
63	Record	Recovery_Employment Services	Integer		PROVIDED SERVICE
64	Record	Recovery_Benefit Planning	Integer		PROVIDED SERVICE
65	Record	Recovery_Peer Recovery Supporter	Integer		PROVIDED SERVICE
66	Record	Recovery_Transportation	Integer		PROVIDED SERVICE
67	Record	Recovery_Prison In Reach	Integer		PROVIDED SERVICE
68	Record	Recovery_Life Skills	Integer		PROVIDED SERVICE
69	Record	Recovery_Relapse Prevention Recovery Checkups	Integer		PROVIDED SERVICE
70	Record	Recovery_Spiritual Support	Integer		PROVIDED SERVICE
71	Record	Recovery_Identification Fund	Integer		PROVIDED SERVICE
72	Record	Recovery_Other please specified	char (100)		PROVIDED SERVICE Brief description of services
73	Record	Record_Notes	char (300)		

B- OhioMHAS CTP User Roles & Responsibilities

Permissions	OhioMHAS Admin	OhioMHAS User	Regional User
Can assign any access level to another access level	Yes		
Search and manage all CTP Users (System Wide)	Yes		
Export all system data to Excel format	Yes		
Create, read, and Update CTP Client Records System wide	Yes	Yes	
Create, read, and Update CTP Client Records by Assigned Region	Yes	Yes	Yes
Can activate all inactive client records	Yes	Yes	Yes
Search and View CTP Client data system wide	Yes	Yes	
Search and View CTP Client data by assigned region	Yes	Yes	Yes
Export Search results for CTP Client data	Yes	Yes	Yes
Run and print reports	Yes	Yes	Yes
Search and view user access logs	Yes		
Export Search results for user access logs	Yes		

C- Business and Functional Requirements

ID	Category	Requirement	Type	Priority
1	User Access	The system will give the administrator the ability to create and manage both remote and State users	Functional	P1 (Must Have)
2	User Access	The system will have the ability to allow the OhioMHAS administrator to manage user access and roles	Functional	P1 (Must Have)
3	User Access	The system will have the ability to authenticate internal state users using their State User ID against the ID Domain Management System.	Functional	P1 (Must Have)
4	Login	System will lock-out user for fifteen minutes after five unsuccessful attempts to log-in.	Functional	P1 (Must Have)
5	Registration	The System will not allow duplicate usernames.	Functional	P1 (Must Have)
6	Login / Password	The system will have the ability for remote users, not State Users, to self-manage their passwords and lost passwords.	Functional	P1 (Must Have)
7	User Access	The system will have the ability to log user access, accessing clients records, and record updates	Functional	P1 (Must Have)
8	User Logs	The system will have the ability for the OCCC Administrator to search the user logs and see: Date Time stamp of access Name of user User Location User actions Updated Client Record	Functional	P1 (Must Have)
9	CTP Application	The system will have the ability to create, read, and update a Client record	Functional	P1 (Must Have)
10	CTP Application	The system will limit a Coordinator to view only client records within their assigned region.	Functional	P1 (Must Have)
11	CTP Application	The system will have the ability to maintain the history of a volunteer through multiple treatment programs. (Client can start-stop-start treatments)	Functional	P1 (Must Have)
12	Search Data	The system will have the ability to search a CTP Record either for system wide records, or by assigned region; data filters include; Client ID Number Last Name First Name Region Client Date of Birth Coordinator Staff Member who inputted application Treatment Type (Provided Service) Date range of treatments Client Status Fiscal Year	Functional	P1 (Must Have)
13	Export CTP Application Records	The system will have the ability to export CTP Search Results to an Excel format	Functional	P1 (Must Have)

ID	Category	Requirement	Type	Priority
14	Export CTP Application Records	The system will allow the OhioMHAS Administrator to download all files and data into an Excel format file	Functional	P1 (Must Have)
15	Reports	The system will have the ability to create and manage reports for (1) Treatments by region (2) Treatment types by month and region	Functional	P1 (Must Have)
16	Manage Tables	System administrator has the ability to update Provided Services data values	Functional	P1 (Must Have)
17	Manage Tables	System administrator has the ability to reassign counties to a different region	Functional	P1 (Must Have)
18	System Browser Compatibility	Firefox 33.11, Safari 51.x, Google Chrome 42, Firefox 6, IE 10,11	Non-Functional	P1 (Must Have)
19	Data Security	System must have the ability to secure and/or encrypt Privacy Health Information / HIPAA as per Ohio Revised Code 1347.15 http://codes.ohio.gov/orc/1347.15	Non-Functional	P1 (Must Have)
20	Manuals	User manual needs to be created for this application	Non-Functional	P1 (Must Have)
21	Manuals	Technical Manual needs to be created for this application	Non-Functional	P1 (Must Have)

D- Additional Requirements

1. Applicable Standards
 - a. Data Retention
 - i. System data will be retained indefinitely
2. Platform Requirements
 - a. Browser Compatibility:
 - i. Firefox 33.11, Safari 51.x, Google Chrome 42, Firefox 6, IE 10,11
 - b. Remote User Password Configuration
 - i. Passwords must be complex
 - ii. Passwords must contain characters from the following categories:
 1. Base 10 digits (0 - 9)
 2. Non-alphanumeric, such as: !@#\$%^&*()_+|\`' " []><.,/?
 3. English uppercase or lowercase (A/a - Z/z)
 4. Must be a minimum of 8 characters
 - iii. No reuse of the last five passwords associated with account
3. Performance Requirements
 - a. The web pages shall fully paint in an average response time of 3 seconds or less over a broad band (DSL or cable) Internet connection.
4. Expected Hours of Availability
 - a. The system will be available except during scheduled maintenance. High usage will be during normal business hours of Monday-Friday 7am-6pm EST.
5. Disaster Recovery
 - a. System data will be backed up once each business day.
6. Policy Compliance
 - a. The system will be compliance with State policies
 - i. Security Policies - B Series
 - ii. Security policy for Protected Health Information (PHI) Data Per Ohio Revised Code 1347.15 / <http://codes.ohio.gov/orc/1347.15>
 - iii. Internet/Intranet Policies - F Series
 - iv. The policies are located at:
(<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx>)
7. Capacity Requirements
 - a. Approximately 50 to 100 User Count
 - b. There are three OhioMHAS Users
 - c. Daily access by six regions with 3+ users per region
8. Transaction Count
 - a. Expect 400-500 new client records per month
 - b. Daily access by OhioMHAS staff members

E - Reports

Report Name	CLIENT RELEASE TYPE	
Date	User Selects Date Range for Report	
Filter	Can filter by Region or by Counties	
Column	DataID	Additional Information
Region	Region (3)	Group by Region
Detainer	Prison Release Type (42)	Total Count by Region Grand Total Count
EDS	Prison Release Type (42)	Total Count by Region Grand Total Count
EST	Prison Release Type (42)	Total Count by Region Grand Total Count
Judicial Release	Prison Release Type (42)	Total Count by Region Grand Total Count
Parole	Prison Release Type (42)	Total Count by Region Grand Total Count
PRC	Prison Release Type (42)	Total Count by Region Grand Total Count
Transitional Control	Prison Release Type (42)	Total Count by Region Grand Total Count
Other	Prison Release Type (42)	Total Count by Region Grand Total Count

Report Name	INSURANCE TYPE	
Date	User Selects Date Range for Report	
Filter	Can filter by Region or by Counties	
Column	DataID	Additional Information
Region	Region (3)	Group by Region
Medicaid	Insurance Type (46)	Total Count by Region Grand Total Count
Private	Insurance Type (46)	Total Count by Region Grand Total Count
Military	Insurance Type (46)	Total Count by Region Grand Total Count
Medicare	Insurance Type (46)	Total Count by Region Grand Total Count
Other	Insurance Type (46)	Total Count by Region Grand Total Count
Uninsured	Insurance Type (46)	Total Count by Region Grand Total Count

Report Name	CLIENT TREATMENT	
Date	User Selects Date Range for Report	
Filter	Can filter by Region or by Counties	
Column	DataID	Additional Information
Region	Region (3)	Group by Region
ClientID	ClientID (9)	Total Sum by Region Grand Total Sum
Treatment_Diagnostic Assessment	Treatment_Diagnostic Assessment (52)	Total Sum by Region Grand Total Sum
Treatment_Intensive outpatient services	Treatment_Intensive outpatient services (53)	Total Sum by Region Grand Total Sum
Treatment_Urinalysis	Treatment_Urinalysis (54)	Total Sum by Region Grand Total Sum
Treatment_Outpatient Treatment	Treatment_Outpatient Treatment (55)	Total Sum by Region Grand Total Sum
Treatment_Community Residential Treatment	Treatment_Community Residential Treatment (56)	Total Sum by Region Grand Total Sum
Treatment_Case Management	Treatment_Case Management (57)	Total Sum by Region Grand Total Sum
Treatment_Medication assisted Treatment	Treatment_Medication assisted Treatment (58)	Total Sum by Region Grand Total Sum
Treatment_Crisis Intervention	Treatment_Crisis Intervention (59)	Total Sum by Region Grand Total Sum
Treatment_Ambulatory detoxification services	Treatment_Ambulatory detoxification services (60)	Total Sum by Region Grand Total Sum
Treatment_Other services	Treatment_Other services (61)	Total Sum by Region Grand Total Sum

Report Name	CLIENT RECOVERY	
Date	User Selects Date Range for Report	
Filter	Can filter by Region or by Counties	
Column	DataID	Additional Information
Region	Region (3)	Group by Region
ClientID	ClientID (9)	Total Sum by Region Grand Total Sum
Recovery_Recovery Housing	Recovery_Recovery Housing (62)	Total Sum by Region Grand Total Sum
Recovery_Employment Services	Recovery_Employment Services (63)	Total Sum by Region Grand Total Sum
Recovery_Benefit Planning	Recovery_Benefit Planning (64)	Total Sum by Region Grand Total Sum
Recovery_Peer Recovery Supporter	Recovery_Peer Recovery Supporter (65)	Total Sum by Region Grand Total Sum
Recovery_Transportation	Recovery_Transportation (66)	Total Sum by Region Grand Total Sum
Recovery_Prison In_Reach	Recovery_Prison In_Reach (67)	Total Sum by Region Grand Total Sum
Recovery_Life Skills	Recovery_Life Skills (68)	Total Sum by Region Grand Total Sum
Recovery_Relapse Prevention Recovery Checkups	Recovery_Relapse Prevention Recovery Checkups (69)	Total Sum by Region Grand Total Sum
Recovery_Spiritual Support	Recovery_Spiritual Support (70)	Total Sum by Region Grand Total Sum
Recovery_Identification Fund	Recovery_Identification Fund (71)	Total Sum by Region Grand Total Sum
Recovery_Other please specified	Recovery_Other please specified (72)	Total Sum by Region Grand Total Sum

Report Name	CLIENT STATUS	
Date	User Selects Date Range for Report	
Filter	Can filter by Region or by Counties	
Column	DataID	Additional Information
Client Region	Client Region (22.2)	Group by Region
Client County	Client County (22.1)	Group County
ClientID	ClientID (9)	
Enrolled	ClientStatus (38)	Total Sum Enrolled By County Total Sum Enrolled by Region Grand Total Sum
Discharged	ClientStatus (38)	Total Sum Discharged By County Total Sum Discharged by Region Grand Total Sum

F- OhioMHAS CTP Data Entity Diagram



Supplement 1

Supplement: Security and Privacy

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 Contractor's 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 excludes sending, taking or making available remotely (directly or indirectly), any State information including 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.